An Internet publication may be considered a "printed publication" within the meaning of 35 U.S.C. § 102(a), but "the one who wishes to characterize the information, in whatever form it may be, as a 'printed publication' ... should produce sufficient proof of its dissemination or that it has otherwise been accessible to persons concerned with the art to which the document relates and thus most likely to avail themselves of its contents." (citations omitted) *In re Wyer*, 210 USPQ 790, 795 (CCPA 1981).

The Kahan reference cited by the Examiner is a paper that was presented at the INET '95 Conference Proceedings held on June 27-30, 1995, in Honolulu, Hawaii. Attachment A is the INET '95 Conference Program which on page 6 shows that J. Kahan presented <u>A Distributed Authorization Model for WWW</u> on June 28, 1995. Indeed, J. Kahan's personal website, a copy of which is enclosed as Attachment B, on page 2 cites the on-line reference as "J. Kahan, A distributed authorization model for WWW, In *INET'95*, June 1995." Thus, it is clear that the paper was presented on June 28, 1995 at the INET '95 Conference and that the author of the paper cites the INET '95 Conference when referencing his paper. However, the question remains as to whether the paper was disseminated or accessible to those persons concerned with the art to which the document relates before its presentation at the INET '95 Conference.

If one follows the hyperlink under the description of the paper on Attachment B, they are taken to a page entitled "Abstract – A Distribution Authorization Model for WWW," a copy of which is enclosed as Attachment C. Attachment C was allegedly "last updated" on August 7, 1995. If one presses the "Up" icon on Attachment C, they are taken to the "Table of Contents: INET'95 Hypermedia Proceedings," a copy of which is enclosed as Attachment D. Attachment D was also allegedly "last updated" on August 7, 1995.

Returning to Attachment C, if one presses the "Full Paper" icon, they are taken to the reference cited by the Examiner, which states that the paper was "last updated" on May 5, 1995. However, there is no indication that the corresponding paper was accessible or made available to those skilled in the art prior to the paper's presentation at the June 28, 1995, INET '95 Conference. If one presses the icon represented by a printer on the "Abstract" page (Attachment C), they are taken to Attachment E which is a PostScript or formatted version of the reference. Attachment E indicates, at the top of each page, that the paper was part of the INET '95 Proceedings. Thus, it is clear that the paper was first <u>presented</u> to those skilled in the art at the INET '95 Conference

Proceedings on June 28, 1995. Further, Attachments C and D, both of which indicate that they were updated as late as August 7, 1995, provide the only "gateway" to the reference cited by the Examiner. The Examiner has provided no proof the reference was accessible anytime before August 7, 1995 (i.e., the last update for the pages leading to the reference).

Applicants disagree with the Examiner's assertion that the reference was published on May 5, 1995. Applicants enclose a copy of the Author Information from the INET '95 Conference as Attachment F. The Author Information contains instructions for updating the author's paper via file transfer protocol (FTP). The "last updated" line at the top of the reference is merely a part of the HTML document which has been added to indicated the date and time at which the author submitted their last update, presumably via FTP. The "last updated" line does not indicate that the paper was disseminated or otherwise accessible to anyone over the Internet or any other means.

In *Carella v. Starlight Archery*, an anticipatory mailer was prepared prior to Applicant's filing date, but there was no evidence as to when the mailer was received by any of the addressees and the magazine containing the mailer was not even mailed until ten day after Applicant's filing date. See *Carella v. Starlight Archery*, 231 USPQ 644, 646-647 (CCPA 1986). Thus, the court held that since there was no evidence that the mailer "was known or used by, or was otherwise accessible to, the public until after the mailing," there was no anticipation. *Id.*

The facts are the same with respect to the *Kahan* reference and the present application. There may be evidence that suggests that the *Kahan* reference was prepared prior to Applicants' effective filing date. However, the Examiner has failed to produce sufficient proof of its dissemination or that it was otherwise accessible to persons concerned with the art to which the document relates before the presentation on June 28, 1995. Accordingly, the *Kahan* reference is not prior art under 35 U.S.C. § 102(a) with respect to the present application.

All of the pending claims are rejected over *Kahan* either alone or in combination with other references. Since Kahan is not prior art with respect to the claimed invention, the rejections of the pending claims must be withdrawn.

In light of the preceding remarks, Applicants submit that all of the pending claims are in condition for allowance and request that the Examiner allow the application to issue. However,

if there are any remaining issues the Examiner is encourage to call Applicant's attorney, Jeffrey H. Canfield at (312) 807-4233 in order to facilitate a speedy disposition of the present case.

If any additional fees are required in connection with this response, they may be charged to deposit account no. 02-1818.

Respectfully submitted,

BELL, BOYD & LLOYD LLC

BY ______________________

Jeffrey H. Canfield
Reg. No. 38,404
P.O. Box 1135
Chicago, Illinois 60690-1135
Phone: (312) 807-4233

[Help] *Last update at http://inet.nttam.com*[redacted]

[redacted]

[redacted]

Conference Program : Overview

[redacted]

9:00-17:00 TUTORIALS at Sheraton Waikiki Hotel

1. Publishing with the World Wide Web
   Alan Emtage, Bunyip, Canada (bajan@bunyip.com)
2. IPng: The Next Generation Internet Protocol
   Steve Deering, Xerox PARC, USA (deering@parc.xerox.com)
3. Internet: Making the Business Case
   Gordon Howell, Internet Business Services, Scotland (gordon@ibs.co.uk)
4. Internetworking with ATM(Asynchronous Transfer Mode)
   Allison Mankin, ISI, USA (mankin@isi.edu)
5. Internet Security
   Steve Crocker, CyberCash, USA (crocker@cybercash.com)

17:00-18:00 Internet Society Open Members Meeting at Sheraton Waikiki Hotel

18:00-20:00 Opening Reception at Sheraton Waikiki Hotel

Wednesday, 28 June 1995

8:30-10:30 L1. Opening Plenary Session
Chair: Eric Schmidt (schmidt@eng.sun.com)

1. **From Conference Chair**
   Eric Schmidt (schmidt@eng.sun.com)
2. **From Governor of Hawaii**
   Benjamin J. Cayetano
3. **From Internet Society**
   Vint Cerf (cerf@isoc.org)
   Larry Landweber (lhl@cs.wisc.edu)
4. **From Program Chairs**
   Kilnam Chon (chon@cosmos.kaist.ac.kr)
   Dan Lynch (dlynch@interop.com)
5. **Note on Conference Proceedings**
   Kilnam Chon (chon@cosmos.kaist.ac.kr)
6. **Keynote Speech: The Global Telecommunication Infrastructure and the Information Society**
   Jean Jipguep, ITU (JEAN.JIPGUEP@itu.ch)

11:00-12:30 PARALLEL BREAKOUT SESSIONS
12:30-14:00--Lunch
14:00-15:30 PARALLEL BREAKOUT SESSIONS
15:30-16:00 BREAK
16:00-17:30/18:00 PARALLEL BREAKOUT SESSIONS
19:00-22:30--LUAU

Thursday, 29 June 1995

8:30-10:30 L2. INET Plenary Session
Chair: David Lassner (david@oit.hawaii.edu)

1. **Keynote Speech: The Evolution and Revolution of the Web**
   Tim Berners-Lee, W3C (timbl@w3.org)

2. **INET Panel : Network Security: Do You Know Who's Breaking in Right Now?**
   Moderator: Gage, John (Sun)
   Panelist: Patrick, John (IBM)
   Panelist: Giordano, Rose Ann (DEC)
   Panelist: Shimomura, Tsutomu (SDSC)
   Panelist: Cerf, Vint (MCI)
   Panelist: Best, Reginald (3COM)

10:30-11:00 Break
11:00-12:30 PARALLEL BREAKOUT SESSIONS
12:30-14:00 Lunch
14:00-15:30 PARALLEL BREAKOUT SESSIONS
15:30-16:00 BREAK
16:00-17:30/18:00 PARALLEL BREAKOUT SESSIONS
18:30-19:30 Cocktail Party

Friday, 30 June 1995

8:30-10:00 PARALLEL BREAKOUT SESSIONS
10:00-10:30--BREAK
10:30-12:30 L3. Closing Plenary Session
Chair: Dan Lynch (dlynch@interop.com)

1. **Keynote Speech: Economic Opportunity Along the Information Superhighway**
   Jonathan Sallet, DoC, USA
2. **Keynote Speech : Internet and Consumer Electronics: Proposed Scenario for Internet Becoming Third Media after Telephone and Television**
   Kazuhiko Nishi, ASCII, Japan (nishi@ascii.co.jp)
3. **INET'96**
   Andy Bjerring, CANARIE, Canada (bjerring@canarie.ca)
4. **Internet 1996 World Exposition**
   Carl Malamud, Internet Multicasting Service, USA (carl@radio.com)
5. **Closing Remarks**
   Eric Schmidt (schmidt@eng.sun.com)

Detailed Conference Program

Tuesday, 27 June 1995

9:00-17:00 TUTORIALS at Sheraton Waikiki Hotel

1. Publishing with the World Wide Web
   Alan Emtage, Bunyip, Canada (bajan@bunyip.com)
2. IPng: The Next Generation Internet Protocol
   Steve Deering, Xerox PARC, USA (deering@parc.xerox.com)
3. Internet: Making the Business Case
   Gordon Howell, Internet Business Services, Scotland (gordon@ibs.co.uk)
4. Internetworking with ATM(Asynchronous Transfer Mode)
   Allison Mankin, ISI, USA (mankin@isi.edu)
5. Internet Security
   Steve Crocker, CyberCash, USA (crocker@cybercash.com)

17:00-18:00 Internet Society Open Members Meeting at Sheraton Waikiki Hotel

18:00-20:00 Opening Reception at Sheraton Waikiki Hotel

[redacted]

8:30-10:30 L1. Opening Plenary Session
Chair: Eric Schmidt (schmidt@eng.sun.com)

1. **From Conference Chair**
   Eric Schmidt (schmidt@eng.sun.com)

2. **From Governor of Hawaii**
   Benjamin J. Cayetano
3. **From Internet Society**
   Vint Cerf (cerf@isoc.org)
   Larry Landweber (lhl@cs.wisc.edu)
4. **From Program Chairs**
   Kilnam Chon (chon@cosmos.kaist.ac.kr)
   Dan Lynch (dlynch@interop.com)
5. **Note on Conference Proceedings**
   Kilnam Chon (chon@cosmos.kaist.ac.kr)
6. **Keynote Speech: The Global Telecommunication Infrastructure and the Information Society**
   Jean Jipguep, ITU (JEAN.JIPGUEP@itu.ch)

11:00-12:30 PARALLEL BREAKOUT SESSIONS

A1: Information Space Environments at Kauai Room
Chair: Schatz, Bruce (schatz@csl.ncsa.uiuc.edu)

1. Maintaining Link Consistency in Distributed Hyperwebs
   Kappe, Frank (fkappe@iicm.tu-graz.ac.at)
2. Interchange of Structured Multimedia Documents Containing External Information
   Acebron, Jose Jesus (acebron@ac.upc.es)
   Delgado, Jaime (delgado@ac.upc.es)
3. Experiences with On-line access to Chemical Journals
   Kirstein, Peter (P.Kirstein@cs.ucl.ac.uk)
   Montasser-Kohsari, Goli (G.MontasserKohsari@cs.ucl.ac.uk)

D1: New Partnerships for Educational Networking at Royal Hawaiian Hotel
Chair: Rutkowski, Kathy (kmr@chaos.com)

1. Building a Commercial Internet Service for Education: Learning from One Vendor's Experience
   Perlman, Richard (rdperlm@pacbell.com)
2. Common Ground: Community Networks as Catalysts
   Klingenstein, Ken (Ken.Klingenstein@Colorado.edu)
3. Learning With the World Wide Web: Connectivity Alone Will Not Save Education
   Rose, Kimberly (rose5@applelink.apple.com)

N1: Multicasting at Molokai Room
Chair: Deering, Steve (deering@parc.xerox.com)

1. Recent Activities in the MICE Conferencing Project
   Kirstein, Peter (P.Kirstein@cs.ucl.ac.uk)
   Clayman, Stuart (S.Clayman@cs.ucl.ac.uk)
   Handley, Mark (M.Handley@cs.ucl.ac.uk)
   Sasse, Angela (A.Sasse@cs.ucl.ac.uk)
2. A Tool for Configuring Multicast Data Distribution over Global Networks
   Voigt, Robert J. (voigt@ece.nps.navy.mil)
   Barton, Robert J. (barton@ece.nps.navy.mil)
   Shukla, Shridhar B. (shukla@ece.nps.navy.mil)
3. Making the MBone Real
   Thyagarajan, Ajit (ajit@ee.udel.edu)
   Casner, Stephen (casner@isi.edu)
   Deering, Steve (deering@parc.xerox.com)

P1: GII and its Relationship to the Internet - Panel at Maui Room
Chair: Kuo, Frank (kuo@ai.sri.com)

1. GII and its Relationship to the Internet (Panel)
   Kuo, Frank (kuo@ai.sri.com)
   Kahn, Robert (rkahn@cnri.reston.va.us)
   Kumon, Shumpei (shumpei@glocom.ac.jp)
   Baser, Robert (BaserR@cp.ic.gc.ca)
   Bjerring, Andrew (bjerring@canarie.ca)

R1: Developing Countries at Honolulu Room
Chair: Lawrie, Mike (mlawrie@frd.ac.za)

1. Research and Academic Networks: The Emerging Tower of Babel
   Lerch, Irving A. (lerchi@acfcluster.nyu.edu)
2. The Sustainable Development Networking Programme: Concept and Implementation
   Zambrano, Raul (zambrano@undp.org)
   Daudpota, Isa (daudpota@sdnpk.undp.org)
3. The International Science Foundation Telecommunications Program
   Mafter, Ilya (Ilya@nwu.edu)
   Shkarupin, Vyacheslav (slava@prs.isf.kiev.ua)

T1: Security at Lanai Room
Chair: Huitema, Christian (huitema@sophia.inria.fr)
1. Secure TCP -- Providing Security Functions in TCP Layer
   Tsutsumi, Toshiyuki (tutumi@ori.hitachi-sk.co.jp)
   Yamaguchi, Suguru (suguru@is.aist-nara.ac.jp)
2. Measured Interference of Security Mechanisms with Network Performance
   Claffy, K. (kc@upeksa.sdsc.edu)
   Braun, Hans-Werner (hwb@upeksa.sdsc.edu)
   Gross, Andrew (grossa@sdsc.edu)

U1: Innovative Designs for Users at Waianae Room
Chair: Foster, Jill (jill.foster@newcastle.ac.uk)
1. User-Oriented Listserv Operation: A Case Study of PHNLINK
   Kim, Sara (sarakim@u.washington.edu)
2. Virtual Museums: Enjoy the Monumentale Cemetery of Milano through the Internet
   Padula, Marco (padula@nerve.itim.mi.cnr.it)
   Celati, A.
   Palumbo, L.
   Negroni, E.
   Perucca, M.
   Rinaldi, G. Rubbia
3. Collaboratory : A Virtual Community
   Watts, Margit Misangyi (watts@uhunix.uhcc.hawaii.edu)

12:30-14:00--Lunch

14:00-15:30 PARALLEL BREAKOUT SESSIONS

A2: Low Bandwidth and Wireless Applications at Kauai Room
Chair: Gerla, Mario (gerla@cs.ucla.edu)
1. Multimedia Message Distribution in a Constrained Environment
   Wijesoma, W. S. (sardha@cse.mrt.ac.lk)
   Fernando, M. S. D. (shantha@infolabs.is.lk)
   Dias, G. V. (gihan@cse.mrt.ac.lk)
2. Extending the Reach of the Internet through Paging
   Dias, Dileeka (dileeka@infolabs.is.lk)
   Dias, Gihan (gihan@infolabs.is.lk)
   Perera, Upul
3. A Remote Robotics Laboratory on the Internet
   Cao, Y. U. (yu@cs.ucla.edu)
   Chen, T.-W. (tsuwei@cs.ucla.edu)
   Harris, M. (mharris@cs.ucla.edu)
   Kahng, A. B. (abk@cs.ucla.edu)
   Lewis, M. A. (tlewis@cs.ucla.edu)
   Stechert, A. D. (andre@cs.ucla.edu)

D2: Internetworking and Educational Reform at Royal Hawaiian Hotel
Chair: Parker, Tracy LaQuey (tparker@cisco.com)
1. Internetworking and Educational Reform: The National School Network Testbed
   Hunter, Beverly (bhunter@bbn.com)
2. A Transformation of Learning: Use of the NII for Education and Lifelong Learning
   Bracey, Bonnie (bbracey@aol.com)
3. Common Knowledge: Pittsburgh
   Carlitz, Robert D. (rdc@vms.cis.pitt.edu)

Zinga, Mario (zinga@pps.pgh.pa.us)

N2: Routing and Addressing at Molokai Room
Chair: Mankin, Allison (mankin@isi.edu)

1. The Routing Arbiter in the Post-NSFnet Service World
   Manning, Bill (bmanning@isi.edu)
2. Problems and Solutions of Dynamic Host Configuration Protocol (DHCP)
   Tominaga, Akihiro (tomy@sfc.wide.ad.jp)
   Nakamura, Osamu (osamu@sfc.wide.ad.jp)
   Teraoka, Fumio (tera@csl.sony.co.jp)
   Murai, Jun (jun@sfc.wide.ad.jp)
3. Stratum-Based Aggregation of Routing Information
   Rekhter, Yakov (yakov@watson.ibm.com)

P2: Democracy at Lanai Room
Chair: Vystavil, Martin (vystavil@savba.sk)

1. Internet: Supporting Democratic Changes in the Post-Communist Slovak Republic
   Vystavil, Martin (vystavil@savba.sk)
2. Democracy and Network Interconnectivity
   Kedzie, Christopher R. (kedzie@rand.org)
3. The Internet and Grassroots Democracy: The Telecommunications Policy Roundtable of the Northeast USA (TPR-NE)
   Klein, Hans (hkklein@mit.edu)

R2: Funding Models at Honolulu Room
Chair: Ozgit, Attila (ozgit@knidos.cc.metu.edu.tr)

1. Networking the Caribbean Region via the Virgin Islands Paradise FreeNet
   de Blanc, Peter (pdeblanc@usvi.net)
2. Turkish Internet (TR-NET) Project: Policies for Organizational Framework and Funding
   Cagiltay, Kursat (kursat@knidos.cc.metu.edu.tr)
   Ozgit, Attila (ozgit@knidos.cc.metu.edu.tr)
   Taner, Erdal (erdal@metu.edu.tr)
   Ozlu, Ufuk (ufuk@kalkan.tetm.tubitak.gov.tr)
   Cakir, Serhat (serhat@kalkan.tetm.tubitak.gov.tr)
3. REUNA: How an Academic Network can be Self-Funded
   Utreras, Florencio (futreras@reuna.cl)

T2: Internet Protocol: Next Generation at Maui Room
Chair: Hinden, Robert (hinden@ipsilon.com)

1. Internet Protocol: Next Generation (Panel)
   Hinden, Bob (hinden@ipsilon.com)
   Bradner, Scott (sob@harvard.edu)
   Deering, Steve (deering@parc.xerox.com)
   Zhang, Lixia (lixia@parc.xerox.com)

U2: Museum at Waianae Room
Chair: George, St. (stgeorge@nsf.gov)

1. Artists on the Internet
   Bishop, Ann (abishop@uiuc.edu)
   Squier, Joseph (joseph@ux1.cso.uiuc.edu)
2. Building On-Ramps to the Information Superhighway: Designing, Implementing and Using Local Museum Infrastructure
   Helfrich, Paul M. (helfrich@fi.edu)
3. Bringing Museums On Line
   Mannoni, Bruno (mannoni@culture.fr)

A3: Distributed Systems at Niihau Room
Chair: Minden, Gary (GMinden@arpa.mil)

1. A Scalable, Deployable, Directory Service Framework for the Internet
   Howes, Timothy A. (tim@umich.edu)
   Smith, Mark C. (mcs@umich.edu)
2. NetAgent: A Global Search System over Internet Resources by Distributed Agents
   Park, Taeha (taeha@nuri.net)

Chon, Kilnam (chon@cosmos.kaist.ac.kr)
3. The UNITE Project: Distributed Delivery and Contribution of Multimedia Objects over the Internet
   Deniau, Cedric (deniau@eecs.ukans.edu)
   Swink, Michael (swink@eecs.ukans.edu)
   Aust, Ron (aust@kuhub.cc.ukans.edu)
   Evans, Joe (evans@eecs.ukans.edu)
   Gauch, Susan (sgauch@tisl.ukans.edu)
   Miller, Jim (miller@eecs.ukans.edu)

15:30-16:00 BREAK

16:00-17:30/18:00 PARALLEL BREAKOUT SESSIONS

A4: Security at Kauai Room
[redacted]

6/28/95

2. Using Public Key Technology -- Issues of Binding and Protection
   Galvin, James M. (galvin@tis.com)
   Murphy, Sandra L. (murphy@tis.com)
3. Simple Key-Management for Internet Protocol (SKIP)
   Aziz, Ashar (ashar.aziz@eng.sun.com)
   Patterson, Martin (martin.patterson@france.sun.com)
   Baehr, Geoff (geoffrey.baehr@eng.sun.com)

D3: New Initiatives To Support School Networking at Royal Hawaiian Hotel
Chair: Smith, Jane (jane.smith@cnidr.org)
1. Internet for Schools - the Singapore Experience
   Tan, Eng Pheng (eptan@moe.ac.sg)
2. Construct Computerized Campus to Lay the NII Foundation
   Tseng, Shian-Shyong (sstseng@cis.nctu.edu.tw)
   Lu, Ai-chin (lu@moers2.edu.tw)
   Yin, Ching-Hai (yin@moers2.edu.tw)
   Chen, Yu-Hsuan (candy@moers2.edu.tw)
3. Summary of K12 Activities in Japan
   Goto, Kunio (goto@nanzan-u.ac.jp)
   Nakayama, Masaya (nakayama@nc.u-tokyo.ac.jp)
4. Setting up a Computer Mediated Communication Network for Secondary Schools
   Cagiltay, Kursat (kursat@knidos.cc.metu.edu.tr)
   Ozgit, Attila (ozgit@knidos.cc.metu.edu.tr)
   Askar, Petek (askarp@rorqual.cc.metu.edu.tr)
5. The Educational Demands of Networking Development in Lithuania
   Reklaitis, Vytautas (vytas@pit.ktu.lt)
   Strom, Jim (j.strom@doc.mmu.ac.uk)

N3: Network Management at Molokai Room
Chair: Huizer, Erik (erik.huizer@surfnet.nl)
1. Producing Quality Factors of LAN Interconnection Services
   Valimaa, Harri (Harri.Valimaa@tele.fi)
   Honkanen, Tapani (Tapani.Honkanen@tele.fi)
2. Preventing Rather than Repairing - A New Approach in ATM Network Management
   Schuhknecht, Anja (schuhknecht@lrz-muenchen.de)
   Dreo, Gabi (dreo@lrz-muenchen.de)
3. Improved Network Management Using NMW (Network Management Worm) System
   Ohno, Hiroyuki (hohno@is.titech.ac.jp)
   Shimizu, Akihiro (akihiro@is.titech.ac.jp)
4. Object Evaluator Management Function
   Choi, Taesang (choits@cstp.umkc.edu)
   Choi, Deokjai (dchoi@cctr.umkc.edu)
   Tang, Adrian (tang@cstp.umkc.edu)

P3: Law and Fair Use at Maui Room
Chair: Civille, Richard (rciville@civicnet.org)

1. Laws of Electronic Communities and Their Roads: High Noon?
   Harter, Peter (pfh@nptn.org)
2. Non-Profit Public Access Network Services (PANS) and Local Internet Service Providers (ISPs): Complement or Conflict?
   Civille, Richard (rciville@civicnet.org)
3. The Law and the Internet : Emerging Legal Issues
   Appelman, Daniel J. (dan@hewm.com)

R3: Networks as Empowering Technology at Honolulu Room
Chair: Hahn, Saul (shahn@umd5.umd.edu)
1. Japan Window: A US-Japan Internet/WWW Collaboration for Japanese Information
   Lee, Burton H. (blee@kiku.stanford.edu)
   Goto, Atsuhiro (atsuhiro@nttam.com)
   Bayle, Michael L. (bayle@fuji.stanford.edu)
   Sakamoto, Yasuhisa (sakamoto@nttam.com)
   Thibeaux, Jeremy (thibeaux@cs.stanford.edu)
2. Friends and Partners: Building Global Community on the Internet
   Cole, Greg (gcole@solar.rtd.utk.edu)
   Bulashova, Natasha (natasha@ibpm.serpukhov.su)
3. Information-Transfer Stations for Developing Countries in Asia
   Smith, Jeff (asianet@well.sf.ca.us)
4. Building A French Virtual Community On Internet: The Example of Frognet
   Oudet, Bruno (bao@access.digex.net)

T3: Alternative Access Technologies at Lanai Room
Chair: Shimojo, Shinji (shimojo@center.osaka-u.ac.jp)
1. Mobility Support in IPv6 Based on the VIP Mechanism
   Teraoka, Fumio (tera@csl.sony.co.jp)
   Uehara, Keisuke (kei@wide.ad.jp)
2. The Internet in Developing Countries: Issues and Alternatives
   Pitke, M. V. (pitke@tifrvax.tifr.res.in)
3. A Data and Telecommunications Gateway between the Internet and ISDN
   Knight, Graham (knight@cs.ucl.ac.uk)
   Bhatti, Saleem N. (S.Bhatti@cs.ucl.ac.uk)
   Clayman, Stuart (S.Clayman@cs.ucl.ac.uk)
4. Fast Packet Technologies in the Internet Environment
   Mohta, Pushpendra (pushp@cerf.net)

U3: Public Health and Medicine at Waianae Room
Chair: Akazawa, S. (akazawa@who.ch)
1. The Global Health Network
   LaPorte, Ronald (rlaporte@vms.cis.pitt.edu)
2. NIH/NLM World Wide Web Database Projects
   Rodgers, R. P. C. (rodgers@nlm.nih.gov)
3. Hospital Information System and the Internet
   Ohe, Kazuhiko (kohe@hcc.h.u-tokyo.ac.jp)
   Kaihara, Shigekoto (kaihara-jyo@h.u-tokyo.ac.jp)
   Ishikawa, Koichi Benjamin (kishikaw@ncc.go.jp)
   Hishiki, Teruyoshi (hishiki-jyo@h.u-tokyo.ac.jp)
   Nagase, Toshiko (nagase-jyo@h.u-tokyo.ac.jp)
   Sakurai, Tunetaro (sakurai-jyo@h.u-tokyo.ac.jp)
4. The Internet and the Genome Project
   Jacobson, Dan (danj@gdb.org)

D4: Using Networks for Collaborative Learning at Niihau Room
Chair: Huston, Michele (michele.huston@anu.edu.au)
1. Slovak Academic Network (SANET) and European Schools Project (ESP) in Slovakia
   Weis, Tibor (tibor@tuzvo.sk)
   Krajnak, Julius (krajnak@tuzvo.sk)
2. Educational Projects Using Networks in Chilean Elementary Schools
   Laval, Ernesto (elaval@enlaces.ufro.cl)
   Flores, Laura (lflores@enlaces.ufro.cl)
3. Constructing Japanese K-12 Network Community: Case Study

Shintani, Takashi (shintani@glocom.ac.jp)
Uchimura, Takeshi (uchimura1@applelink.apple.com)
4. The ACTEIN Program: Bringing the Internet to Australian Schools
Huston, Michele (michele.huston@anu.edu.au)
5. Development of WWW Services in Mexico, Toward a National Information Infrastructure
Fernandez, Jeffry (jeff@jeff.dca.udg.mx)

19:00-22:30--LUAU

Thursday, 29 June 1995

8:30-10:30 L2. INET Plenary Session
Chair: David Lassner (david@oit.hawaii.edu)
1. **Keynote Speech: The Evolution and Revolution of the Web**
Tim Berners-Lee, W3C (timbl@w3.org)
2. **INET Panel : Network Security: Do You Know Who's Breaking in Right Now?**
Moderator: Gage, John (Sun)
Panelist: Patrick, John (IBM)
Panelist: Giordano, Rose Ann (DEC)
Panelist: Shimomura, Tsutomu (SDSC)
Panelist: Cerf, Vint (MCI)
Panelist: Best, Reginald (3COM)

10:30-11:00 Break

11:00-12:30 PARALLEL BREAKOUT SESSIONS

A5: Navigating the Web at Kauai Room
Chair: Bogen, Manfred (Manfred.Bogen@gmd.de)
1. The User Interface of URLs
Hoffman, Paul E. (phoffman@proper.com)
2. Searching Internet Resources Using IP Multicast
Kashima, Hiroaki (kashima@csce.kyushu-u.ac.jp)
Ishida, Yoshiki (yoshiki@cc.kyushu-u.ac.jp)
Furukawa, Zengo (zengo@ec.kyushu-u.ac.jp)
Ushijima, Kazuo (ushijima@csce.kyushu-u.ac.jp)
3. Document Management, Digital Libraries and the Web
Masinter, Larry (masinter@parc.xerox.com)

C1: The Internet for Business at Molokai Room
Chair: Agoston, Tom (agoston@vnet.ibm.com)
1. Publishing Models for Internet Commerce
O'Reilly, Tim (tim@ora.com)
2. Launching Internet Services in Asia: The Hong Kong Experience
Wong, Pindar (pindar@hk.super.net)
3. Daiichi Advanced Home Shopping Structure on the Internet
Matsumoto, Toshifumi (matsumoto@spin.ad.jp)
Senoo, Yoshitaka (senoo@daiichi.co.jp)

D5: Building New Global Learning Communities at Royal Hawaiian Hotel
Chair: Maak, Laurie (lmaak@netcom.com)
1. YouthCaN
Clements, Millard (clements@acf6.nyu.edu)
2. APICNET: A Japanese Initiative to Create a Global Classroom on the Internet
Tsubo, Toshi (tsubo@apic.or.jp)
Kaneko, Yoko (kaneko@apic.or.jp)
Pavonarius, Richard (richard@apic.or.jp)
Sekiguchi, Mikiko (mikiko@apic.or.jp)
Matsumoto, Toshifumi (matsumoto@spin.ad.jp)
3. Creating Global Learning Communities: I*EARN's Action-Based Projects
Brown, Kristin (krbrown@igc.apc.org)

N4: Scaling the Internet Up - Panel at Maui Room

Chair: Gross, Phil (6423401@mcimail.com)
1. Scaling the Internet Up (Panel)
   Gross, Phil (6423401@mcimail.com)
   Li, Tony
   Bradner, Scott
   Rekhter, Yakov

P4: Economics and Pricing at Niihau Room
Chair: Perez, Miguel (mperez@lascar.puc.cl)
1. Public Policies to Encourage High-Speed Residential Internet Access
   Gillett, Sharon Eisner (sharon@far.mit.edu)
2. Internet Economics: What Happens When Constituencies Collide
   Bailey, Joseph (bailey@rpcp.mit.edu)
   McKnight, Lee (mcknight@rpcp.mit.edu)
3. Pricing the Internet : A Model and a Practical Implementation.
   Perez, Miguel A. (mperez@lascar.puc.cl)

R4: Pacific at Honolulu Room
Chair: Lassner, David (david@hawaii.edu)
1. Enehana Kamepiula - Computer Telecommunication for a Hawaiian Speaking Generation
   Donaghy, Keola (keola@maui.com)
2. Self-Determination in the Information Age
   Crawford, Scott P. (exec@hawaii-nation.org)
   Crawford, Kekula P. B. (kekula@hawaii-nation.org)
3. Internet Services via PEACESAT
   Okamura, Norman (norman@elele.peacesat.hawaii.edu)
   Blake, Al (alb@ffa.gov.sb)
   Lam, Reuben (rlam@elele.peacesat.hawaii.edu)
   Mukaida, Lori (lmukaida@elele.peacesat.hawaii.edu)

U4: Enterprise Networking at Waianae Room
Chair: Weider, Chris (clw@bunyip.com)
1. Internet Affects the Corporation: Experiences from Eight Years of Connectivity
   Johnson, Suzanne M. (johnson@intel.com)
2. Internet Usage Guidelines in a Commercial Setting
   Trio, Nicholas (nrt@watson.ibm.com)
   Patrick, John (jrp@vnet.ibm.com)

T4: High Performance Networking at Lanai Room
Chair: Kim, Dae Young (dykim@comsun.chungnam.ac.kr)
1. Solutions of IPng Support for Wireless-ATM Integration
   Lu, Wai (ddke0002@utmkl.bitnet)
2. Internetworking with ATM-Based Switched Virtual Networks
   Ghane, Kamran (kamran@neda.com)
3. The Failure of Conservative Congestion Control in Large Bandwidth-Delay Product Networks
   Kim, Hyogon (hkim@dsl.cis.upenn.edu)
   Farber, David J. (farber@central.cis.upenn.edu)

12:30-14:00 Lunch

14:00-15:30 PARALLEL BREAKOUT SESSIONS

A6: Engineering the Web at Kauai Room
Chair: Berners-Lee, Tim (timbl@w3.org)
1. Supporting a URI Infrastructure by Message Broadcasting
   Freitas, Vasco (vf@uminho.pt)
   Rio, Miguel (rio@uminho.pt)
   Costa, Antonio (costa@uminho.pt)
   Macedo, Joaquim (macedo@uminho.pt)
2. Schizophrenic HTTP Server
   Barrett, Alan P. (barrett@ee.und.ac.za)
3. Intelligent Caching for WWW Objects

Wessels, Duane (wessels@colorado.edu)

D6: New Concepts of Learning at Royal Hawaiian Hotel
Chair: Perlman, Richard (rdperlm@pacbell.com)

1. MegaMath: Expanding and Connecting the Mathematics Community
   Casey, Nancy (casey931@cs.uidaho.edu)
2. The Internet and K-12 Mathematics and Science Reform
   Thomas, David (dave@mathfs.math.montana.edu)
   Stevenson, Stephanie (stevens@mail.fim.edu)
3. Science Education as a Driver of Cyberspace Technology Development
   Pea, Roy (pea@nwu.edu)
   Gomez, Louis (gomez@covis.nwu.edu)
   Edelson, Daniel (edelson@covis.nwu.edu)

N5: High Speed Networking at Molokai Room
Chair: Rekhter, Yakov (yakov@watson.ibm.com)

1. TCP/IP on Gigabit Networks
   Wilson, Anne (awilson@chernikeeff.co.uk)
2. Multimedia Experiments at the University of Pisa: From Videoconference to Random Fractals
   Giordano, Stefano (giordano@iet.unipi.it)
   Russo, Franco (russo@iet.unipi.it)
   Pierazzini, Giuseppe (peppe@pisa.infn.it)
3. Traffic Measurements in Multimedia Documents Real Time Transfer
   Lancia, Maurizio (lancia@iasi.rm.cnr.it)
   Gaibisso, Carlo (gaibisso@iasi.rm.cnr.it)
   Biondi, Vincenzo (biondi@iasi.rm.cnr.it)
   Gambosi, Giorgio (gambosi@mat.utovrm.it)
   Vitale, Maurizio (vitale@iasi.rm.cnr.it)

P5: Public Interest Regulation - Panel at Niihau Room
Chair: McClaughlin, Sean (seanm@hawaii.edu)

1. Public Interest Regulation (Panel)
   McLaughlin, Sean (seanm@Hawaii.Edu)
   Goto-Sabas, Jennifer (71532.3261@compuserve.com)
   Naito, Yukio (71532.3261@compuserve.com)
   Fukunaga, Carol (carolf@kalama.doe.hawaii.edu)
   Johanson, Cindy (cjohanson@pbs.org)
   Boutilier, Sybil (citylink@well.com)

R5: Asia at Honolulu Room
Chair: Narayan, Devendra (narayan@sut.ac.jp)

1. Connecting China Education Community to the Global Internet - The China Education and Research Network Project
   Li, Xing (xing@cernet.edu.cn)
   Wu, Jianping (jianping@cernet.edu.cn)
   Liang, Youneng (liangyn@tsinghua.edu.cn)
2. Asia Now Online
   Zoughlin, Malia (malia@uhunix.uhcc.hawaii.edu)
3. Pan Asia Networking: A Strategic Framework - Concepts, Goals, and Operations
   Wilson, Paul (pwilson@peg.apc.org)
   Hoon, Maria Ng Lee (MARIANGLEEHOON@idrc.org.sg)
   Garton, Andrew (agarton@peg.apc.org)

C2: Electronic Money at Lanai Room
Chair: Coggeshall, Bob (coggs@hongkong.cogwheel.com)

1. Using the Internet to Reduce Software Piracy
   Hauser, Ralf C. (hauser@acm.org)
2. Digital Cash and Monetary Freedom
   Matonis, Jon W. (74774.3663@compuserve.com)
3. CyberCash: Payments Systems for the Internet
   Crocker, Stephen (crocker@cybercash.com)
   Boesch, Brian (boesch@cybercash.com)
   Hart, Alden (ahart@cybercash.com)

Lum, James (jimlum@cybercash.com)

U5: Networked Information Discovery and Retrieval - Panel at Maui Room
Chair: Lynch, Cliff (clifford.lynch@ucop.edu)

1. Networked Information Discovery and Retrieval Technologies (Panel)
   Lynch, Cliff (clifford.lynch@ucop.edu)
   Michelson, Avra (avram@mitre.org)
   Preston, Cecilia (cpreston@info.berkeley.edu)
   Summerhill, Craig (craig@cni.org)

P6: Government Services at Waianae Room
Chair: Searle, Gregory (searle@tdg.uoguelph.ca)

1. Building Community Computer Networks for All Canadians: Public Ownership, Access and Communication on the Information Highway
   Searle, Gregory (searle@tdg.uoguelph.ca)
   Richardson, Don (drichard@uoguelph.ca)
   Stevenson, John (jsteven@alcor.concordia.ca)
2. The World Wide Web and Its Implications in a Democratic Society
   Doyle, Pattie (pidoyle@tdc.redstone.army.mil)
   Ross, Angela S. (aross@tdc.redstone.army.mil)
   Edwards, Rita R. (redwards@tdc.redstone.army.mil)
3. Future Prospects for NSF's International Connections Program Activities
   Goldstein, Steven N. (goldste@nsf.gov)

15:30-16:00 BREAK

16:00-17:30/18:00 PARALLEL BREAKOUT SESSIONS

A7: Infrastructure for Networked Applications - Panel at Maui Room
Chair: Leiner, Barry (bleiner@arpa.mil)

1. Infrastructure for Networked Applications (PANEL)
   Leiner, Barry (bleiner@arpa.mil)
   Huitema, Christian (huitema@sophia.inria.fr)
   Huizer, Erik (erik.huizer@surfnet.nl)
   Kummerfeld, Bob (bob@cs.su.oz.au)
   Schatz, Bruce (schatz@csl.ncsa.uiuc.edu)

D7: New Applications of Networking Technology for Education at Royal Hawaiian Hotel
Chair: Rutkowski, Kathy (kmr@chaos.com)

1. Educational Application of the Internet: International Joint Teleclass
   Aoki, Kumiko (kaoki@uhunix.uhcc.hawaii.edu)
   Goto, Kunio (goto@nanzan-u.ac.jp)
2. Net-Frog: Using the WWW to Learn about Frog Dissection and Anatomy
   Kinzie, Mable B. (Kinzie@virginia.edu)
   Larsen, Valerie A. (vl5q@virginia.edu)
   Burch, Joeseph B. (jbb@virginia.edu)
   Boker, Steven M. (boker@virginia.edu)
3. Data Exchange and Telecollaboration -- Technology in Support of New Models of Education
   Feldman, Alan (alan_feldman@terc.edu)
   Allen, Irene (irene_allen@terc.edu)
   Johnson, Lisa (lisa_johnson@terc.edu)
   Lieberman, Daniel (daniel_lieberman@terc.edu)
   Hoeven, Johan van der (johan_van_der_hoeven@terc.edu)
4. Analyzing Linkage Structure in a Course-Integrated Virtual Learning Community on the World Wide Web

   James, Leon (leon@uhunix.uhcc.hawaii.edu)
   Bogan, Kevin (bogan@uhunix.uhcc.hawaii.edu)
5. Creating Online Interactive Educational Environments: Lessons Learned from the NASA K-12 Internet Initiative
   Hodas, Steven (hodas@nsipo.nasa.gov)
   Seigel, Marc (msiegel@quest.arc.nasa.gov)

N6: High Speed Wide Area Networks at Molokai Room

Chair: Wilson, Ann (acw@chernikeeff.ac.uk)

1. Real Use of the SuperJanet High Speed Multiservice Network
   Dyer, John (John.Dyer@ukerna.ac.uk)
2. The Implementation of a High Speed Network for the DFN-Community
   Kaufmann, Peter (kaufmann@dfn.d400.de)
3. Towards a European High-Speed Backbone
   Behringer, Michael (M.H.Behringer@dante.org.uk)
4. Post-NSFNET Statistics Collection
   Claffy, K. (kc@upeksa.sdsc.edu)
   Braun, Hans-Werner (hwb@upeksa.sdsc.edu)

P7: Transborder Information Flows at Niihau Room
Chair: Peng, H.A. (mcmangph@leonis.nus.sg)

1. Internet Policy Issues in New Zealand
   Jackson, Colin (colin.jackson@comms.moc.govt.nz)
2. Censorship and the Internet: A Singapore Perspective
   Ang, Peng Hwa (mcmangph@leonis.nus.sg)
   Nadarajan, Berlinda
3. Issues in the Transborder Flow of Scientific Data
   Uhlir, Paul F. (puhlir@nas.edu)
   Alexander, Shelton S. (shel@geosc.psu.edu)

R6: Europe at Honolulu Room
Chair: Bakonyi, Peter (h25bak@ella.hu)

1. The SANET Network: Further Evolution
   Gajdos, Peter (gajdos@uakom.sk)
2. UNIBEL: Academic and Research Network of Belarus
   Kritsky, Sergei (kritsky@ok.minsk.by)
   Ivanov, Andrey (ivanov@ok.minsk.by)
   Listopad, Nikolay (listopad@cacedu.minsk.by)
3. Kiev Pilot IP Network
   Shkarupin, Viacheslav Slava (slava@prs.isf.kiev.ua)
   Demchenko, Yuri (demch@nicc.polytech.kiev.ua)
4. RUNNet - Federal University Network of Russia
   Vasilyev, Vladimir N. (vasilev@ipmo.spb.su)
   Gugel, Yuri V. (gugel@ifmo.ru)
   Kirchin, Yuri G. (kirchin@ifmo.ru)
   Robachevsky, Andrei M. (andrei@ifmo.ru)
5. Romanian National Computer Network for Research and Higher Education
   Staicut, Eugenie (estaicut@roearn.ici.ro)
   Popa, Julian (julian@roearn.ici.ro)
   Macri, George (gmacri@roearn.ici.ro)
   Toia, Adrian (atoia@roearn.ici.ro)
6. Bringing Internet to North-West of Russia -- RUSNet N/W project
   Zaborovski, Vladimir (vlad@stu.spb.su)
   Lopota, Vitaly (vlopota@stu.spb.su)
   Shemanin, Yuri (yuri@fuzzy.stu.neva.ru)
   Tarasov, Stanislav (star@stu.spb.su)

C3: Business of the Internet at Lanai Room
Chair: Takahashi, Toru (toru@tokyonet.ad.jp)

1. Tourism Promotion Using the World Wide Web
   Lennon, Martin (mlennon@chcsn1.ait.ac.nz)
2. The Internet for Small Businesses: An Enabling Infrastructure for Competitiveness
   Poon, Simpson (spoon@swin.edu.au)
   Swatman, Paula (pswatman@ponderosa.is.monash.edu.au)
3. Commercial Use of the Internet
   Levitt, Lee (levitt@process.com)

U6: Community Networking at Waianae Room
Chair: Bishop, Ann (abishop@uiuc.edu)

1. Networked Ocean Science Research and Education, Monterey Bay California
   Brutzman, Don (brutzman@nps.navy.mil)

2. Enhancing Communication and Cooperation in Human Service Delivery through the Internet
   Young, Maree
   Milosevic, Zoran (zoran@cs.uq.oz.au)
3. Potential Users and Virtual Communities in the Academic World
   Silvio, Jose (j.silvio@unesco.org)
4. Energy Utilities in the Internet and NII: Users or Providers?
   Aiken, Robert J. (aiken@es.net)
   Cavallini, John S. (cavallini@nersc.gov)
   Scott, Mary Ann (scott@er.doe.gov)

P8: Internet Privacy Guideline - Panel at Kauai Room
Chair: Rotenberg, Marc (rotenberg@epic.org)

1. Internet Privacy Guideline (Panel)
   Burrington, Bill (billburr@aol.com)
   Baser, Robert (BaserR@cp.ic.gc.ca)
   Tuerkheimer, Frank (fmtuerkh@facstaff.wisc.edu)
   Calvo, Rafael Fernandez (rfcalvo@guest2.atimdr.es)

18:30-19:30 Cocktail Party

Friday, 30 June 1995

8:30-10:00 PARALLEL BREAKOUT SESSIONS

A8: Multimedia Interface to Cyberspace at Maui Room
Chair: Kummerfeld, Bob (bob@cs.su.oz.au)

1. MMMGate - Enabling Overall Multimedia Messaging
   Bogen, Manfred (Manfred.Bogen@gmd.de)
   Krechel, Arnold (Arnold.Krechel@gmd.de)
2. Reliable Audio for Use over the Internet
   Hardman, Vicky (v.hardman@cs.ucl.ac.uk)
   Sasse, Angela (a.sasse@cs.ucl.ac.uk)
   Handley, Mark (m.handley@cs.ucl.ac.uk)
   Watson, Anna (a.watson@cs.ucl.ac.uk)
3. Use of Audio and Video on the Internet
   Muirden, Richard (richard@rmit.edu.au)

D8: Professional Development and Training at Royal Hawaiian Hotel
Chair: Huston, Michele (michele@aarnet.edu.au)

1. Teachers and Internet: Charting a Course for Success
   Buchanan, Phil (p.buchanan@mailbox.uq.oz.au)
2. Training is for Dogs: Teachers Teach; Teachers Learn
   Murray, Janet (jmurray@psg.com)
3. Blazing a Path to the Internet
   Joseph, Linda C. (ljoseph@magnus.acs.ohio-state.edu)

N7: Network Information Centers at Molokai Room
Chair: Conrad, David (davidc@keio.jp.apnic.net)

1. Financing Common Infrastructure
   Schachtner, Andreas (afs@germany.eu.net)
2. JPNIC: A Country NIC for Administrating Common Network Resources and Providing Network Information in Japan
   Hirabaru, Masaki (hi@nic.ad.jp)
   Takada, Hiroaki (hiro@nic.ad.jp)
   Nakayama, Masaya (nakayama@nic.ad.jp)
   Murai, Jun (jun@nic.ad.jp)
3. Network Skills in a Networked Information World: The Latest Tips and Tools
   Calcari, Susan (susanc@internic.net)

P9: Industrial Policy at Niihau Room
Chair: Klein, Hans (hkklein@mit.edu)

1. Measuring and Comparing the Return on Investment on Network-Related Empowerment

Ruth, Stephen (ruth@gmu.edu)
2. Surf's Up! Hawaii Attempts to Develop an Information Industry and Statewide Internetwork But Doesn't Always Catch the Right Wave
   Harkness, Stephen (stephen@ptc.org)

R7: Americas at Honolulu Room
Chair: Reich, Ricardo (rreich@halcon.dpi.udec.cl)
1. Empowering Information Professionals and End Users with New Cultural Values
   Ferreiro, Soledad (sferreir@abello.seci.uchile.cl)
2. Networking In Latin America and the Caribbean and the OAS/RedHUCyT Project
   Hahn, Saul (shahn@umd5.umd.edu)
3. STARNET/IP : A Commercial Approach to Internet
   Torres, Eduardo Jose (torrese@infomail.infonet.com)

C4: Future of Commerce on the Net at Lanai Room
Chair: Mitchell, Keith (keith@pipex.net)
1. The Emerging Internet Market
   Howell, Gordon (gordon@ibs.co.uk)
   Weir, George R. S. (gw@cs.strath.ac.uk)
   Freeth, Tony (tony@ibs.co.uk)
2. Internet: Improving the Actual Benefit and Reducing the (Hidden) Cost
   Veenis, Joop (jve@tg.nl)
3. Electronic Commerce on Internet: What Is Still Missing?
   Milosevic, Zoran (zoran@cs.uq.oz.au)
   Bond, Andy (bond@dstc.edu.au)

R8: Middle East/North Africa at Waianae Room
Chair: El Sherif, Hisham (hsherif@ritsec.com.eg)
1. The Communication Infrastructure and the Internet Services as a Base
   Kamel, Tarek (tkamel@ritsec.com.eg)
   Baki, Nashwa Abdel (nashwa@frcu.eun.eg)
2. Internet's Role in Middle-East Development: Palestinian Perspective
   Zougbi, Saleem G. (saleem@bethlehem.edu)
3. Jordan's National Information System
   Nusseir, Yousef (j_nic@ritsec.com.eg)
4. Networking Efforts in the Maghreb Region
   Sellami, Khaled (sellami@irsit.mrt.tn)

10:00-10:30--BREAK
10:30-12:30 L3. Closing Plenary Session
Chair: Dan Lynch (dlynch@interop.com)
1. **Keynote Speech: Economic Opportunity Along the Information Superhighway**
   Jonathan Sallet, DoC, USA
2. **Keynote Speech : Internet and Consumer Electronics: Proposed Scenario for Internet Becoming Third Media after Telephone and Television**
   Kazuhiko Nishi, ASCII, Japan (nishi@ascii.co.jp)
3. **INET'96**
   Andy Bjerring, CANARIE, Canada (bjerring@canarie.ca)
4. **Internet 1996 World Exposition**
   Carl Malamud, Internet Multicasting Service, USA (carl@radio.com)
5. **Closing Remarks**
   Eric Schmidt (schmidt@eng.sun.com)

Remarks: Room Assignment

Sheraton Waikiki Hotel
    Kauai, Maui, Molokai, Lanai, Niihau, Honolulu, Waianae
Royal Hawaiian Hotel
    Regency

[Back to Top]

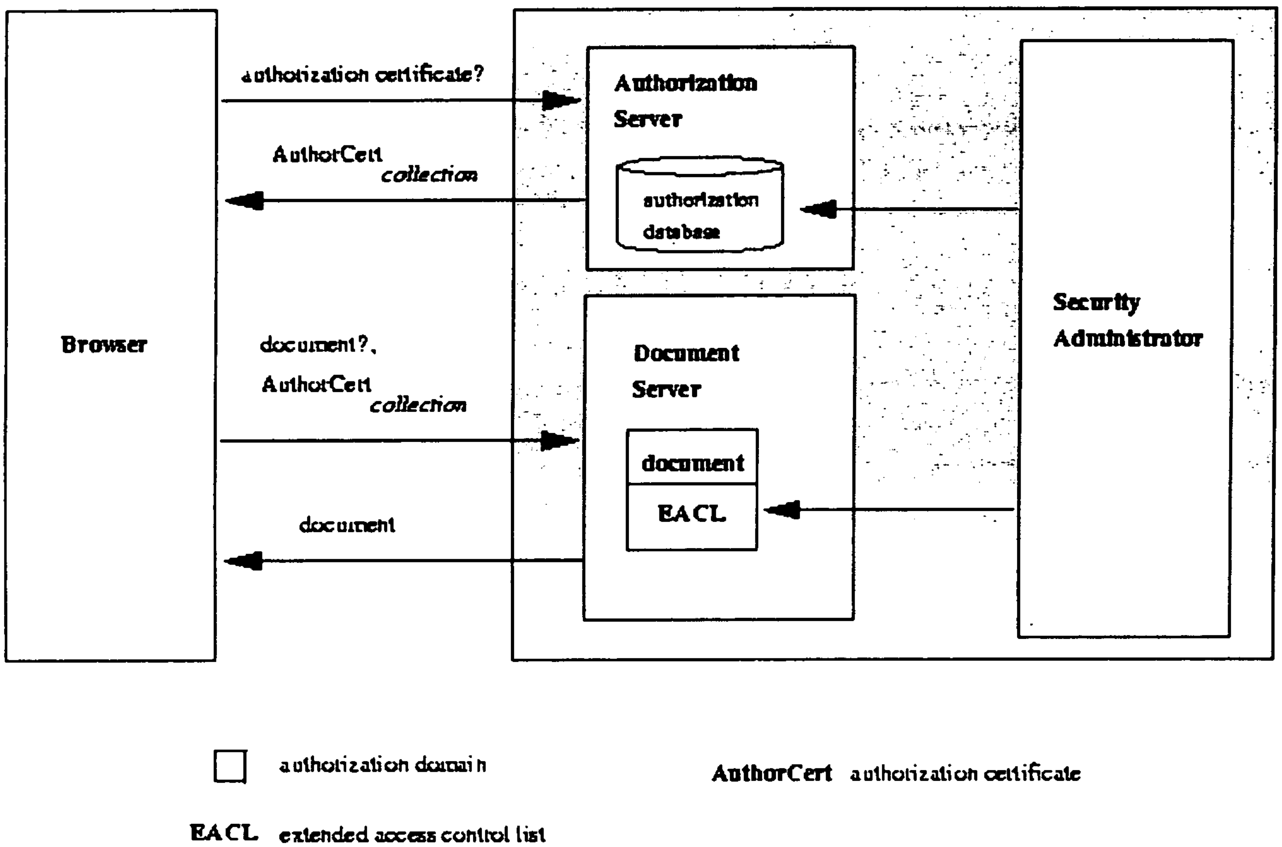
B

DISCLAIMER: this work represents the author's own opinions and not necessarily those of W3C or of INRIA.

WDAI

WDAI is a proposal for a simple and general infrastructure for distributed authorization on the World-Wide Web. Under WDAI, browsers and servers exchange authorization information using X.509v3-based authorization certificates.

Here's a bird's view of WDAI:



The goals of WDAI are the following:

Provide a simple and general authorization infrastructure for distributed hypertext systems

- Support of the hypertext data model (collections, document sharing),
- Offer the tools to let administrators specify their own security policies,
- Simple user administration,
- Minimize the number of data exchanges needed to authenticate and authorize a request..
- W3 compatiblity: compatible with existing protocols and browsers,

and, the most important one,

- Sensibilize more people to the problems of authorization in distributed hypertext systems.

Project history

Oct 1998: Idea for WDAI occurs while attending ApacheCon'98 (Apache developers conference)

May 1998: Paper presented at WWW8: "WDAI: a simple W3 distributed authorization infrastrcture"

Summer 1998 (expected): Tartu, a prototype implementation of WDAI using Apache, mod_ssl, open SSL, and your favorite browser.

Previous work

CAMWWW

CAMWWW is an earlier work I developed during my PhD (to be honest, CAMWWW is the name of the prototype I built, rather of the project, but it's a simple way to refer to it). I developed a non nominative capability-based access control model adapted for distributed hypermedia systems. In CAMWWW, access rights to documents are set up according to the properties of hypertext document collections. Access information is exchanged between browsers and servers using a propietary self-contained capability, inspired from the ECMA-238 standard. I built a prototype using Mosaic/PGP and the NCSA httpd server. My plan was to release it but the NSA (Never Say Anything) put pressure on the NCSA folks and made them retire Mosaic/PGP from the public distribution. Mosaic/PGP was just a patched Mosaic which had hooks for calling PGP or PEM. It didn't include either of those tools, so it was a pity it was "destroyed."

WDAI is different from CAMWWW in that it doesn't impose any security policy and that it can be used with standard SSL-enabled browsers.

Here's some of the on-line references on CAMWWW (I have a couple more, but I don't have time to put all of them here today).

- J. Kahan

  WDAI: a simple World Wide Web distributed authorization infrasutrcture

  In *Proc. WWW'9*, Computer Networks, v. 31, pp. 1599-1609, 1999.

  http://www.ww8.org/w8-papers/4d-electronic/wdai/wdai.html

- J. Kahan,
  Conception et Expérimentation d'un Modèle de Contrôle d'Accès Non Nominatif pour les Systèmes Hypermédia Répartis,
  PhD thesis, Université de Rennes I, December 1997,
  In French. ftp://ftp.irisa.fr/techreports/theses/1997/kahan.ps.gz.

[redacted]

Contributors

... are welcome!

For the moment, I'm the only one working on WDAI and I only work on it during my free time, after work hours.

Contact info

José KAHAN

W3C/INRIA, ZIRST 655, av. de l'Europe, 38330 Montbonnot Saint Martin FRANCE

jose(a)w3.org

José

C

[Help] *Last update at http://inet.nttam.com : Mon Aug 7 21:39:55 1995*

Application Technology
A4: Security

Full Paper

A Distributed Authorization Model for WWW

Kahan Oblatt, Jose  (kahan@ccett.fr)

Abstract

1. PROBLEM AND MOTIVATION

The World-Wide Web (WWW) organizes information into sets of hypertext documents, where a document comprises links to contents and to other documents, rules for the document's presentation, and rules for link-traversal. Documents and contents may be stored in different servers. We use the term node to refer to either a document or a content. We refer to a set of linked documents as a presentation tree. We assume that each presentation tree has a root document.

The use of hypertext structures requires a coordinated authorization approach. Granting access to a document may require granting access to the document's linked contents. Otherwise, a browser could not correctly present the document. Moreover, granting access to a presentation tree may imply granting access to all of the documents that compose the tree. Otherwise, a user would not be able to consult a presentation tree as intended.

Existing WWW authorization schemes are based on Access-Control List (ACL) mechanisms. A document server authorizes a client's request by comparing the client's authenticated identity against the document's ACL, granting the access if the client has an entry which comprises the requested access mode. These schemes present the following drawbacks: (i) a server needs to know its potential clients; and (ii) granting or revocation of access to a document or to a presentation tree requires the modification of the ACLs associated with several nodes. Moreover, the existing schemes do not propose any infrastructure for coordinating the administration of ACLs when the documents are stored in different servers.

2. A CAPABILITY-BASED DISTRIBUTED AUTHORIZATION MODEL

We propose an authorization model which provides authorization at the document and the presentation tree levels. The model organizes document servers into authorization domains. the domain's node servers condition access to their documents to a client's presentation of appropriate capabilities. The two principal assumptions we make are: (i) a domain comprises a global clock; and (ii) a server can authenticate its clients.

The model has two phases. In an installation phase, a security administrator associates with each document a list of capabilities that correspond to the document's outgoing links to other nodes. Moreover, the security administrator generates another list of capabilities for accessing root documents and stores it in an authorization server.

In a consultation phase, the authorization server grants clients delegated capabilities for retrieving root documents. Document servers answer a client's document request with the appropriate document and a delegated version of the document's list of capabilities. The client use these capabilities to retrieve contents and other documents.

In a group extension of the model, each document is associated with an ACL whose entries correspond to the presentation trees that include the document. The authorization server now delegates to clients a group- capability granting access to a presentation tree. To access any document belonging to the presentation tree, the client just needs to present this capability.

Both the model and the group extension take into account the two approaches for document migration on the WWW, namely, the use of redirection addresses, and the use of URL-to-URN name resolvers.

Capabilities comprise attributes which protect them against their unauthorized use, modification, and forgery. Other attributes provide different capability revocation techniques.

3. UTILITY OF THE MODEL

The capability-based authorization model simplifies the security administration of clients as only the authorization server needs to know its clients.

The model allows an easy implementation of need-to-know authorization polices. Indeed, a client only obtains the capabilities necessary to consult a presentation tree and to present the tree's documents.

Moreover, we estimate that the model can be used in contexts where the client population changes at fast rates; for example, an electronic public library where a client buys access for a certain time.

4. VALIDATION OF THE MODEL

We have implemented a prototype of the capability-based authorization model and its group extension over an existing WWW system. The prototype allowed us gave us a valuable insight into how to integrate the model and its performance expectations.

[Archives]

[Help] *Last update at http://inet.nttam.com : Mon Aug 7 21:46:59 1995*

Table of Contents: INET'95 Hypermedia Proceedings

Track Index

Application Technology

[Back to Top]

A1: Information Space Environments
Chair: Schatz, Bruce (schatz@csl.ncsa.uiuc.edu)

1. Maintaining Link Consistency in Distributed Hyperwebs
   Kappe, Frank (fkappe@iicm.tu-graz.ac.at)
2. Interchange of Structured Multimedia Documents Containing External Information
   Acebron, Jose Jesus (acebron@ac.upc.es)
   Delgado, Jaime (delgado@ac.upc.es)
3. Experiences with On-line access to Chemical Journals
   Kirstein, Peter (P.Kirstein@cs.ucl.ac.uk)
   Montasser-Kohsari, Goli (G.MontasserKohsari@cs.ucl.ac.uk)

A2: Low Bandwidth and Wireless Applications
Chair: Gerla, Mario (gerla@cs.ucla.edu)

1. Multimedia Message Distribution in a Constrained Environment
   Wijesoma, W. S. (sardha@cse.mrt.ac.lk)
   Fernando, M. S. D. (shantha@infolabs.is.lk)
   Dias, G. V. (gihan@cse.mrt.ac.lk)
2. Extending the Reach of the Internet through Paging
   Dias, Dileeka (dileeka@infolabs.is.lk)
   Dias, Gihan (gihan@infolabs.is.lk)
   Perera, Upul
3. A Remote Robotics Laboratory on the Internet
   Cao, Y. U. (yu@cs.ucla.edu)
   Chen, T.-W. (tsuwei@cs.ucla.edu)
   Harris, M. (mharris@cs.ucla.edu)
   Kahng, A. B. (abk@cs.ucla.edu)
   Lewis, M. A. (tlewis@cs.ucla.edu)
   Stechert, A. D. (andre@cs.ucla.edu)

A3: Distributed Systems
Chair: Minden, Gary (GMinden@arpa.mil)

1. A Scalable, Deployable, Directory Service Framework for the Internet
   Howes, Timothy A. (tim@umich.edu)
   Smith, Mark C. (mcs@umich.edu)
2. NetAgent: A Global Search System over Internet Resources by Distributed Agents
   Park, Taeha (taeha@nuri.net)

Watson, Anna (a.watson@cs.ucl.ac.uk)

3. Use of Audio and Video on the Internet
   Muirden, Richard (richard@rmit.edu.au)

Commercial and Business Aspect

[Back to Top]

C1: The Internet for Business

Chair: Agoston, Tom (agoston@vnet.ibm.com)

1. Publishing Models for Internet Commerce
   O'Reilly, Tim (tim@ora.com)
2. Launching Internet Services in Asia: The Hong Kong Experience
   Wong, Pindar (pindar@hk.super.net)
3. Daiichi Advanced Home Shopping Structure on the Internet
   Matsumoto, Toshifumi (matsumoto@spin.ad.jp)
   Senoo, Yoshitaka (senoo@daiichi.co.jp)

C2: Electronic Money

Chair: Coggeshall, Bob (coggs@hongkong.cogwheel.com)

1. Using the Internet to Reduce Software Piracy
   Hauser, Ralf C. (hauser@acm.org)
2. Digital Cash and Monetary Freedom
   Matonis, Jon W. (74774.3663@compuserve.com)
3. CyberCash: Payments Systems for the Internet
   Crocker, Stephen (crocker@cybercash.com)
   Boesch, Brian (boesch@cybercash.com)
   Hart, Alden (ahart@cybercash.com)
   Lum, James (jimlum@cybercash.com)

C3: Business of the Internet

Chair: Takahashi, Toru (toru@tokyonet.ad.jp)

1. Tourism Promotion Using the World Wide Web
   Lennon, Martin (mlennon@chcsn1.ait.ac.nz)
2. The Internet for Small Businesses: An Enabling Infrastructure for Competitiveness
   Poon, Simpson (spoon@swin.edu.au)
   Swatman, Paula (pswatman@ponderosa.is.monash.edu.au)
3. Commercial Use of the Internet
   Levitt, Lee (levitt@process.com)

C4: Future of Commerce on the Net

Chair: Mitchell, Keith (keith@pipex.net)

1. The Emerging Internet Market
   Howell, Gordon (gordon@ibs.co.uk)
   Weir, George R. S. (gw@cs.strath.ac.uk)
   Freeth, Tony (tony@ibs.co.uk)
2. Internet: Improving the Actual Benefit and Reducing the (Hidden) Cost
   Veenis, Joop (jve@tg.nl)
3. Electronic Commerce on Internet: What Is Still Missing?
   Milosevic, Zoran (zoran@cs.uq.oz.au)
   Bond, Andy (bond@dstc.edu.au)

Education

[Back to Top]

D1: New Partnerships for Educational Networking

Chair: Rutkowski, Kathy (kmr@chaos.com)

1. Building a Commercial Internet Service for Education: Learning from One Vendor's Experience
   Perlman, Richard (rdperlm@pacbell.com)
2. Common Ground: Community Networks as Catalysts
   Klingenstein, Ken (Ken.Klingenstein@Colorado.edu)
3. Learning With the World Wide Web: Connectivity Alone Will Not Save Education
   Rose, Kimberly (rose5@applelink.apple.com)

D2: Internetworking and Educational Reform

Chair: Parker, Tracy LaQuey (tparker@cisco.com)

Network and Application Engineering

INET'95 [Back to Top]

Policy

[Back to Top]

1. Building Community Computer Networks for All Canadians: Public Ownership, Access and Communication on the Information Highway
   Searle, Gregory (searle@tdg.uoguelph.ca)
   Richardson, Don (drichard@uoguelph.ca)
   Stevenson, John (jsteven@alcor.concordia.ca)
2. The World Wide Web and Its Implications in a Democratic Society
   Doyle, Pattie (pidoyle@tdc.redstone.army.mil)
   Ross, Angela S. (aross@tdc.redstone.army.mil)
   Edwards, Rita R. (redwards@tdc.redstone.army.mil)
3. Future Prospects for NSF's International Connections Program Activities
   Goldstein, Steven N. (goldste@nsf.gov)

P7: Transborder Information Flows
Chair: Peng, H.A. (mcmangph@leonis.nus.sg)

1. Internet Policy Issues in New Zealand
   Jackson, Colin (colin.jackson@comms.moc.govt.nz)
2. Censorship and the Internet: A Singapore Perspective
   Ang, Peng Hwa (mcmangph@leonis.nus.sg)
   Nadarajan, Berlinda
3. Issues in the Transborder Flow of Scientific Data
   Uhlir, Paul F. (puhlir@nas.edu)
   Alexander, Shelton S. (shel@geosc.psu.edu)

P8: Internet Privacy Guideline - Panel
Chair: Rotenberg, Marc (rotenberg@epic.org)

1. Internet Privacy Guideline (Panel)
   Burrington, Bill (billburr@aol.com)
   Baser, Robert (BaserR@cp.ic.gc.ca)
   Tuerkheimer, Frank (fmtuerkh@facstaff.wisc.edu)
   Calvo, Rafael Fernandez (rfcalvo@guest2.atimdr.es)

P9: Industrial Policy
Chair: Klein, Hans (hkklein@mit.edu)

1. Measuring and Comparing the Return on Investment on Network-Related Empowerment
   Ruth, Stephen (ruth@gmu.edu)
2. Surf's Up! Hawaii Attempts to Develop an Information Industry and Statewide Internetwork But Doesn't Always Catch the Right Wave
   Harkness, Stephen (stephen@ptc.org)

Regional

[Back to Top]

R1: Developing Countries
Chair: Lawrie, Mike (mlawrie@frd.ac.za)

1. Research and Academic Networks: The Emerging Tower of Babel
   Lerch, Irving A. (lerchi@acfcluster.nyu.edu)
2. The Sustainable Development Networking Programme: Concept and Implementation
   Zambrano, Raul (zambrano@undp.org)
   Daudpota, Isa (daudpota@sdnpk.undp.org)
3. The International Science Foundation Telecommunications Program
   Mafter, Ilya (Ilya@nwu.edu)
   Shkarupin, Vyacheslav (slava@prs.isf.kiev.ua)

R2: Funding Models
Chair: Ozgit, Attila (ozgit@knidos.cc.metu.edu.tr)

1. Networking the Caribbean Region via the Virgin Islands Paradise FreeNet
   de Blanc, Peter (pdeblanc@usvi.net)
2. Turkish Internet (TR-NET) Project: Policies for Organizational Framework and Funding
   Cagiltay, Kursat (kursat@knidos.cc.metu.edu.tr)
   Ozgit, Attila (ozgit@knidos.cc.metu.edu.tr)
   Taner, Erdal (erdal@metu.edu.tr)
   Ozlu, Ufuk (ufuk@kalkan.tetm.tubitak.gov.tr)
   Cakir, Serhat (serhat@kalkan.tetm.tubitak.gov.tr)

5. Romanian National Computer Network for Research and Higher Education
   Staicut, Eugenie (estaicut@roearn.ici.ro)
   Popa, Julian (julian@roearn.ici.ro)
   Macri, George (gmacri@roearn.ici.ro)
   Toia, Adrian (atoia@roearn.ici.ro)
6. Bringing Internet to North-West of Russia -- RUSNet N/W project
   Zaborovski, Vladimir (vlad@stu.spb.su)
   Lopota, Vitaly (vlopota@stu.spb.su)
   Shemanin, Yuri (yuri@fuzzy.stu.neva.ru)
   Tarasov, Stanislav (star@stu.spb.su)

R7: Americas
Chair: Reich, Ricardo (rreich@halcon.dpi.udec.cl)

1. Empowering Information Professionals and End Users with New Cultural Values
   Ferreiro, Soledad (sferreir@abello.seci.uchile.cl)
2. Networking In Latin America and the Caribbean and the OAS/RedHUCyT Project
   Hahn, Saul (shahn@umd5.umd.edu)
3. STARNET/IP : A Commercial Approach to Internet
   Torres, Eduardo Jose (torrese@infomail.infonet.com)

R8: Middle East/North Africa
Chair: El Sherif, Hisham (hsherif@ritsec.com.eg)

1. The Communication Infrastructure and the Internet Services as a Base
   Kamel, Tarek (tkamel@ritsec.com.eg)
   Baki, Nashwa Abdel (nashwa@frcu.eun.eg)
2. Internet's Role in Middle-East Development: Palestinian Perspective
   Zougbi, Saleem G. (saleem@bethlehem.edu)
3. Jordan's National Information System
   Nusseir, Yousef (j_nic@ritsec.com.eg)
4. Networking Efforts in the Maghreb Region
   Sellami, Khaled (sellami@irsit.rnrt.tn)

Network Technology

[Back to Top]

T1: Security
Chair: Huitema, Christian (huitema@sophia.inria.fr)

1. Secure TCP -- Providing Security Functions in TCP Layer
   Tsutsumi, Toshiyuki (tutumi@ori.hitachi-sk.co.jp)
   Yamaguchi, Suguru (suguru@is.aist-nara.ac.jp)
2. Measured Interference of Security Mechanisms with Network Performance
   Claffy, K. (kc@upeksa.sdsc.edu)
   Braun, Hans-Werner (hwb@upeksa.sdsc.edu)
   Gross, Andrew (grossa@sdsc.edu)

T2: Internet Protocol: Next Generation
Chair: Hinden, Robert (hinden@ipsilon.com)

1. Internet Protocol: Next Generation (Panel)
   Hinden, Bob (hinden@ipsilon.com)
   Bradner, Scott (sob@harvard.edu)
   Deering, Steve (deering@parc.xerox.com)
   Zhang, Lixia (lixia@parc.xerox.com)

T3: Alternative Access Technologies
Chair: Shimojo, Shinji (shimojo@center.osaka-u.ac.jp)

1. Mobility Support in IPv6 Based on the VIP Mechanism
   Teraoka, Fumio (tera@csl.sony.co.jp)
   Uehara, Keisuke (kei@wide.ad.jp)
2. The Internet in Developing Countries: Issues and Alternatives
   Pitke, M. V. (pitke@tifrvax.tifr.res.in)
3. A Data and Telecommunications Gateway between the Internet and ISDN
   Knight, Graham (knight@cs.ucl.ac.uk)
   Bhatti, Saleem N. (S.Bhatti@cs.ucl.ac.uk)

Users

[Back to Top]

Trio, Nicholas (nrt@watson.ibm.com)
Patrick, John (jrp@vnet.ibm.com)

U5: Networked Information Discovery and Retrieval - Panel

Chair: Lynch, Cliff (clifford.lynch@ucop.edu)

1. Networked Information Discovery and Retrieval Technologies (Panel)
   Lynch, Cliff (clifford.lynch@ucop.edu)
   Michelson, Avra (avram@mitre.org)
   Preston, Cecilia (cpreston@info.berkeley.edu)
   Summerhill, Craig (craig@cni.org)

U6: Community Networking

Chair: Bishop, Ann (abishop@uiuc.edu)

1. Networked Ocean Science Research and Education, Monterey Bay California
   Brutzman, Don (brutzman@nps.navy.mil)
2. Enhancing Communication and Cooperation in Human Service Delivery through the Internet
   Young, Maree
   Milosevic, Zoran (zoran@cs.uq.oz.au)
3. Potential Users and Virtual Communities in the Academic World
   Silvio, Jose (j.silvio@unesco.org)
4. Energy Utilities in the Internet and NII: Users or Providers?
   Aiken, Robert J. (aiken@es.net)
   Cavallini, John S. (cavallini@nersc.gov)
   Scott, Mary Ann (scott@er.doe.gov)

[Back to Top]

E

A Distributed Authorization Model for WWW

José Kahan <kahan@ccett.fr>

Abstract

Information in WWW is organized in sets of linked hypertext documents and contents. Both documents and contents can be stored in different servers. We propose a distributed authorization model which provides coordinated authorization to related contents and documents independently of their location. Client administration is simplified as only one server needs to know its potential clients. Document and content servers make local authorization decisions using capabilities presented by their clients. The proposed model comprises sequential and non-sequential access modes. Moreover, the model supports existing WWW node migration techniques.

1 Introduction

The World-Wide Web (WWW) [6] organizes information into sets of hypertext[1] documents, where a document comprises links to media contents, links to other hypertext documents, and rules specifying the presentation of contents and the traversal of links. We refer to a set of related inter-linked documents, such as the sections of this paper, as a *presentation tree*. We refer to the entry point of a presentation tree as a *root document*. Finally, we use the term *node* to refer to either a document or a content.

WWW supports the distribution of nodes by providing node-naming structures (e.g., URLs [5]) and information retrieval protocols (e.g., HTTP [4]). By storing nodes according to their type in specialized servers, the system's overall load and capacity can be better balanced.

The use of hypertext structures requires a coordinated authorization approach. Granting access to a document should also involve granting access to the contents linked to that document. Otherwise, users would not be able to correctly perceive the document. Similarly, granting access to a presentation tree should involve granting access to all the documents that constitute the tree. Otherwise, a user would not be able to consult the presentation tree as intended.

Despite the support of distribution in WWW, little progress has been made in providing coordinated authorization under this context [24]. Existing WWW authorization approaches for distributed nodes are based on Access Control List (ACL) mechanisms [19]. These approaches require either that node servers know their potential clients or that node requests involve a consultation with an authorization server. The former approach presents a client administration problem when the client population changes at a fast rate. The latter approach presents a potential performance bottleneck as the processing of a node request depends on the availability of the authorization server.

The following sections present a distributed authorization model which supports authorization at the presentation tree and document levels for distributed documents and contents. In this model, only one server needs to know its potential clients, while node servers make local authorization decisions using capabilities presented by their clients. The model supports a sequential access mode to presentation trees. An extension to the model provides a non-sequential access mode. Section 2 gives key authorization requirements for the model. Section 3 describes the authorization model. Section 4 presents extensions to support node migration techniques. Section 5 presents a group extension which provides the non-sequential access mode. Section 6 describes our experiences in building a prototype of the model. Section 7 reviews related work in the field. The paper ends with a summary and some perspectives.

2 Authorization requirements

This section gives a brief summary (in no particular order) of the key requirements that have shaped our authorization model.

- *Coordinated authorization.* The model must support authorization at the document and presentation tree levels.
- *Distributed authorization.* To avoid a potential denial of service and to improve response time, it is important that node servers be able to take access control decisions locally, without having to consult other servers.
- *Minimization of the number of servers needing to know their potential clients.* Client

[1] In this paper, we use the terms *hypermedia* and *hypertext* interchangeably; what is said about hypertext also applies to hypermedia.

administration is simplified if few servers have to be contacted to change the status of a client.

- *Support for node sharing.* Documents and presentation trees should be able to reuse existing nodes without compromising authorization.

- *Enforcement of least privilege.* Clients should not receive more privilege than is necessary during a consultation session [20]. That is, granting access to a document should only grant additional access to the contents linked to the document; granting access to a presentation tree should only grant access to the documents that compose the tree.

- *Respect for existing WWW information retrieval protocols.* One of the reasons for the popularity of WWW is the simplicity of its protocols. The model must avoid complicating the existing protocols.

- *Backward compatibility with existing nodes.* It must be possible to control access to existing nodes without having to modify them.

- *Support for node migration.* Because of changes in computer systems and networks, nodes may need to migrate from one server to another. A user who has access rights over an object must always be able to access the object, regardless of the object's migration.

3 A capability-based authorization model

3.1 Overview

The capability-based authorization model groups node servers into *authorization domains.* Clients wishing to retrieve nodes from these servers must include appropriate capabilities [19] in their node requests.

In addition to node servers, an authorization domain comprises a *Security Administrator* (SA), responsible for the generation and installation of capabilities, as well as an *Authorization Server* (AUS), responsible for granting root document capabilities (Figure 1). Although node capabilities share the same format, we distinguish hereafter between a capability for accessing a document (Dcap) and a capability for accessing a content (Ccap) in order to explain the properties of the model.

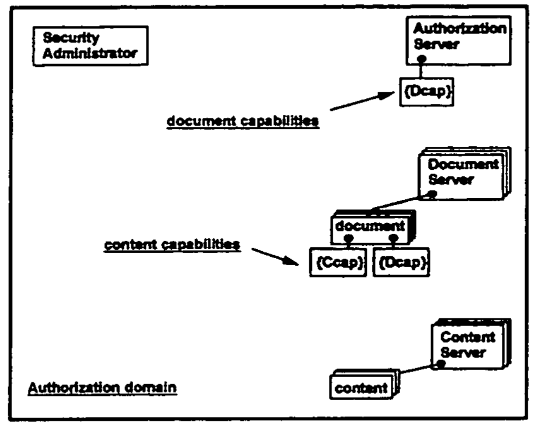


Figure 1: Authorization domain overview

During an installation phase, the SA generates for each document in the domain a list of capabilities which corresponds to the document's outgoing links to other nodes. The SA may follow a *capability association policy* to evaluate whether a capability should be associated with a link. For example, the policy could specify that only links going to children nodes should be taken into account. The SA installs these lists in the node servers that handle the corresponding documents. Moreover, the SA generates a list of capabilities that grant access to the root documents and installs it in the AUS. As the SA is the only entity that can generate new node capabilities, capability control and validation is greatly simplified. A node can be shared among different documents by associating capabilities for that node to those documents.

During a consultation phase, clients acquire nodes and capabilities. The AUS grants clients delegated capabilities for accessing root documents. Document servers grant clients documents and delegated versions of the corresponding lists of capabilities.

The AUS is the only server in the domain that needs to know its potential clients in order to authorize the granting of a capability for a root document. Node servers do not need to know their potential clients; they just require that their clients present appropriate capabilities to be able to authorize the node requests.

A capability includes attributes that allow a node server to validate it locally without needing to consult an additional server. In this way, a node request only involves one server.

The capability assignation scheme imposes a sequential order for document consultation. Section 5 describes a group extension to the model

which allows a non-sequential access to nodes.

The rest of this section describes the assumptions taken in the environment, the properties of capabilities, the message exchanges during the consultation phase, and the limitations of the model.

3.2 Environment assumptions

We assume that in an authorization domain:

- The servers of the domain can synchronize themselves with respect to a trusted, global clock [11];
- Servers can authenticate their clients;
- A node has a unique identifier in the domain; for example, a URL [5];
- Servers have a unique identity;
- A node server knows the identity of its domain's SA and AUS;
- Servers have access to a digital signature [1] mechanism; and
- A server knowing another server's identity can also verify said server's digital signature.

3.3 Properties of capabilities

This section briefly describes the format, generation, delegation, and revocation of capabilities. A previously published article [8] describes further in detail these properties.

Node identifier
Access rights
Validity period
Capability identifier
Grantor server identifier
SA identifier
SA signature

Table 1: Capability attributes

We based the format of the capabilities on that of the privilege attribute certificates (PAC) defined by the standard ECMA-138 [7]. According to this standard, a capability is generated by a *grantor* which then sends it to a *grantee.* Protection of a capability against its unauthorized propagation is achieved by including the grantee's identity inside the capability and requiring grantee authentication during the authorization process. Protection of a capability against its unauthorized use with another target is achieved by including the target's identifier inside the capability. Protection of a capability against its unauthorized modification and forgery is achieved by having the grantor server sign the capability.

Capability
Delegated access rights
Authorizator
Grantor server signature

Table 2: Delegated capability attributes

Table 1 shows the different attributes of a capability. Both the AUS and document servers grant capabilities by means of a delegation operation [23, 17, 15]. Table 2 gives the attributes of a delegated capability. A grantor server proves its right to delegate a capability by signing the delegated capability. A node server can verify this signature using the capability's `grantor server identifier` attribute. In this way, delegated capabilities can self-authenticate grantor servers.

Grantee identifier (GIA)
Validity period
Authorizator identifier
AUS identifier
AUS signature

Table 3: Authorizator attributes

A delegated capability's `authorizator` attribute is a special capability that the AUS generates when delegating a root document capability (Table 3). The authorizator's `grantee identifier` attribute (GIA) specifies the identity with which a client must authenticate itself when using the delegated capability. For instance, the value of the GIA could be an IP network address or a public key [15]. The authorizator's `validity period` attribute indicates the lifetime of a delegated capability.

The AUS is the only domain entity that can generate authorizators. Two reasons lie behind this choice. Firstly, this restriction removes the risk of having a compromised server assign unauthorized lifetimes to its delegated capabilities. Secondly, this restriction diminishes the risk of having a compromised server grant delegated capabilities to an unauthorized client.

During a session, a node server propagates the authorizator from the delegated capability associated with a request to the capabilities it will delegate. As there is only one authorizator per consultation session, the authorizator's `validity period` attribute also indicates the total time available to a client for consulting a presentation tree.

As with all capability-based systems, revocation of capabilities is a major issue. The `validity period` attributes, together with the global clock, guarantee the revocation of capabilities. Moreover, the different identifier attributes can be used to revoke capabilities before their validity expires.

3.4 Consultation phase

This phase comprises three different protocols which allow a client to retrieve a capability for a root document, a document, and a content respectively.

In the following protocols, we use the terms *Request-Node* and *Response-Node* as a shorthand notation for the actual information retrieval protocol data units used by WWW. Moreover, capabilities are distinguished from the WWW protocol data units. Finally, we show the client authentication process as a separate protocol step. The above conventions help illustrate the properties of the protocol and should not be seen as implementation guidelines.

1.	Client to AUS:
	URL of Document + [authorization info]
2.	AUS to Client:
	DDcap

Table 4: Root document capability retrieval

Retrieval of a root document capability. This protocol is as follows (Table 4):

1. The client first requests a root document capability from an authorization server. According to the security policy of the AUS, the client may need to include additional authorization information, such as a password or another capability. The model does not specify the type or values of this parameter.

2. In order to authorize the request, the AUS may use the client's authorization information, the URL of the document document, and any other additional security information which the AUS may have on the client. Having authorized the request, the AUS generates an authorizator and delegates the requested capability. Finally, the server returns the delegated capability to the client (we distinguish delegated capabilities with a letter "D" prefix).

1.	Client to Document Server:
	Authentication according to the GIA
2.	Client to Document Server:
	Request-Document + DDcap
3.	Document Server to Client:
	Response-Document + {DDcap} + {DCcap}

Table 5: Document retrieval

Document retrieval. This protocol allows a client to retrieve a document and the document's associated list of capabilities (Table 5):

1. The client first authenticates to the document server according to the value of the GIA.

2. The client then requests the document adding the appropriate capability to the request.

3. The document server authorizes the request by verifying the integrity and validity of the delegated capability. Moreover, the server compares the authenticated client's identity against the value of the GIA. Having authorized the request, the document server uses the authorizator from the client's delegated capability to delegate the list of capabilities associated to the requested document. The server then returns the document and the delegated capabilities to the client.

1.	Client to Content Server:
	Authentication according to the GIA
2.	Client to Content Server:
	Request-Content + DCcap
3.	Content Server to Client:
	Response-Content

Table 6: Content retrieval

Content retrieval. This protocol is similar to the preceding one with the exception that no delegated capabilities are returned to the client (Table 6). Indeed, contents do not have links to other nodes.

3.5 Limitations

This section briefly describes the main limitations of our authorization model.

- *Document server vulnerability.* As a document server can delegate capabilities, the compromise of this kind of server may affect other node servers.

- *Eventual lack of performance.* To validate a delegated capability, a node server has to

verify three signatures: the SA's signature of the capability, the AUS's signature of the authorizator, and the grantor server's signature of the delegated capability. When requesting a document, one must add to the validation time, the time needed to delegate the document's associated list of capabilities.

- *Regeneration of capabilities.* Whenever the validity period of a capability expires, the SA must regenerate that capability. Moreover, if the SA's signature is compromised, the SA must warn all the node servers belonging to its domain and regenerate all of the existing capabilities.

- *Bookmarks.* It is usual in WWW to copy document's URLs into local bookmark files. In the authorization model, a client can follow a bookmark link to a protected document as long as it has an appropriate capability. Once this capability expires, the bookmark link becomes useless: to obtain a new capability for the same document, the client would need to follow the tree's structure until it reaches the desired document. This limitation may be partially avoided by having the AUS grant capabilities for different documents belonging to a same presentation tree.

- *Evaluation of client consultation time.* The authorizator indicates the total time that a client has for consulting a presentation tree. However, it is not easy to give an estimation of this time: one must consider the user idle time, the workload of the node servers and the network, ... If the authorizator validity period is not correctly evaluated, a client may not be able to travel to all the nodes belonging to a presentation tree.

4 Support for node migration

This section describes how the model may support two existing node migration techniques: node migration by redirection [4], and node migration by use of Uniform Resource Names (URNs) [21, 18]. We assume that the reader is familiar with both techniques.

4.1 Node migration by redirection

In this method, a migrating node leaves a URL for its new location together with a capability for accessing it on the new server (Table 7):

1.	Client to Document Server 1: Authentication according to the GIA
2.	Client to Document Server 1: Request-Document + DDcap
3.	Document Server 1 to Client: URL of Document + DDcap
4.	Client to Document Server 2: Authentication according to the GIA
5.	Client to Document Server 2: Request-Document + DDcap
6.	Document Server 2 to Client: Response-Document + {DDcap} + {DCcap}

Table 7: Node redirection support

1 and 2. A client requests a protected document from document server 1.

3. Document server 1 replies with the document's new URL and a delegated capability for accessing the document at its new location.

4, 5 and 6. The client then uses this capability to request the document from server 2 as described in a precedent section.

A limitation of this method is that each time a node migrates, the retrieval protocol is increased by the first three protocol steps. This is not practical when nodes migrate frequently from one server to another. Another limitation is an increase of the trust placed on content servers: content servers can now grant access to other content servers.

4.2 Use of Uniform Resource Names (URNs)

A URN is a logical reference to a node. *Name servers* provide a resolution of URNs into URLs. This scheme can be integrated into the model by defining a *URN capability* type that, instead of granting access to a node, grants access not only to a node's URL but also to an appropriate capability for requesting that node. Document servers now store URN capabilities along with documents. Name server store node capabilities along with the URLs.

The protocol is as follows (Table 8):

1 and 2. A client requests a protected document from the document server.

3. The document server returns a delegated list of URN capabilities and the document.

4 and 5. Before retrieving a document, the client

1. Client to Document Server:
   Authentication according to the GIA
2. Client to Document Server:
   Request-Document + DDcap
3. Document Server to Client:
   Response-Document + {DURNDcap} + {DURNCcap}
4. Client to Name Server:
   Authentication according to the GIA
5. Client to Name Server:
   URN of Document + DURNDcap
6. Name Server to Client:
   URL of Document + DDcap

Table 8: URN support

contacts the name server to find the document's URL. As with a node request, the client must authenticate itself to the name server and present an appropriate capability.

6. Having authorized the request, the name server returns the URL and a delegated version of the corresponding capability.

A limitation of this method is that both content and name servers must be trusted as they can grant access to other servers. Note that with this method, a client always executes the same number of protocol steps to retrieve a node, regardless of how many times the node has migrated.

5 A group extension

The group extension supports non-sequential access to nodes. Figure 2 shows the modifications to the authorization model.

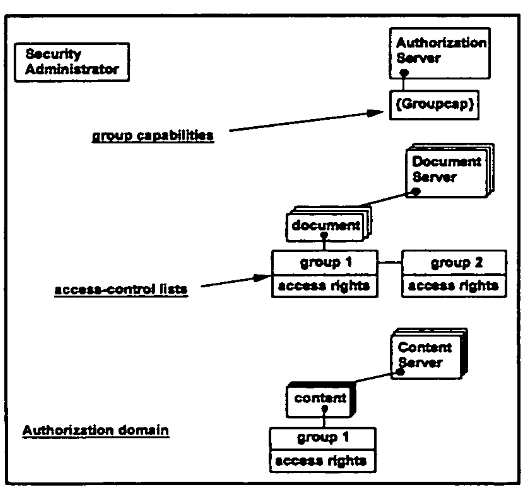


Figure 2: Group support overview

In this extension, each node is associated with an ACL. Each entry of the ACL is a double-tuple which includes a group name and the access rights that the group has over the node. Group names correspond to presentation trees. Thus, all the nodes used in a presentation tree have the same group entry. On the other hand, the entries of a node's ACL correspond to all the presentation trees that use that node. In order to retrieve any of the nodes used in a presentation tree, a client needs to join a *group capability* (Groupcap) to its node requests. A group capability, which is granted by the AUS, gives a client access to a presentation tree for a given time. The format of this capability is the same as the one shown in Table 1, but includes a group name instead of a node identifier.

1. Client to AUS:
   Group Name + [authorization info]
2. AUS to Client:
   DGroupcap
3. Client to Node Server:
   Authentication according to the GIA
4. Client to Node Server:
   Node URL + DGroupcap
5. Node Server to Client:
   Node

Table 9: Group extension protocol

The message exchanges for this protocol are similar to those described in Section 3.4 (Table 9). Document servers do not have to delegate capabilities as the client only needs one group capability to access any node of the tree. To authorize a node request, node servers not only have to validate the capabilities, but they also have to validate the capability and the request against the node's ACL. The group extension is independent of node migration techniques as it merely requires that a migrating node's ACL migrate too.

We shall now discuss how this extension affects the limitations of our model. As a document server no longer delegates capabilities, the compromise of such a server does not affect other node servers. This authorization method is faster than the preceding one as it only requires one delegation operation. A client wishing to follow a bookmark link to a document still needs an appropriate capability. Once the capability expires, the client just needs to acquire a new group capability to reuse the bookmark link. This authorization scheme still requires the evaluation of the client consultation time for a presentation tree. Node migration support does not place any additional trust in content servers or name servers.

The principal limitation of this extension is that each presentation tree needs to have a unique identifier. Another limitation is that the inclusion of an existing node into a presentation tree requires the updating of the node's ACL. Finally, searching a node's ACL may be cumbersome if the node is a component of several presentation trees.

6 Implementation considerations

This section describes the principal choices and problems we have encountered while implementing the model. [9] describes the implementation in further detail.

In order to validate the concepts of the model, we have developed a prototype of the model which includes the node redirection support and the group extension. We chose to build the prototype on NCSA's WWW client (Mosaic 2.4) and server (httpd 2.3) as this system proposes hooks to a PGP/PEM enciphering layer [16]. We used these hooks to "plug-in" an authorization layer to the system. This allowed us to quickly arrive at a working prototype.

The prototype uses the technique described in [15] to implement self-authenticating capabilities. Asymmetric keys are used to sign capabilities as well as to authenticate the grantor servers. The AUS's and SA's public keys are distributed to the node servers during the installation phase. The public keys of grantor servers are used as the value of the capabilities' *grantor server identifier* attribute, and are thus distributed inside the capabilities. Grantor servers use their private keys to sign the capabilities which they delegate as proof of their identity. Thus, each delegated capability contains the signature of a grantor server and the public key which allows to verify the signature.

A similar technique is used to authenticate clients. Clients uses their private keys to sign every request they make. When a client requests a capability from the AUS, the client includes in the request its identity and the root document's URL. In order to authenticate the client, the AUS must retrieve the client's public key from a local file or from a key certification center. Having authorized the request, the AUS creates an authorizator using the the client's public key as the value of the GIA. As the client's public key is distributed inside the authorizator, node servers can authenticate the client without having to contact other servers.

The above technique can be modified to minimize the use of a client's public key. In this variation, the AUS creates a session asymmetric key pair and uses the session public key as the value of the GIA. The AUS first enciphers the session private key using the client's public key and then sends it together with the delegated capability to the client. Thereafter, the client uses the session private key to sign its requests. The session key pair remains valid during the lifetime of the authorizator.

To exchange capabilities between clients and servers, we added a header to the HTTP messages. The drawback of this method is that the client had to be modified so that it could add and remove capabilities to and from messages. [3] proposes an alternative method whereby capabilities are exchanged inside documents. In this method, document servers embed each of a document's delegated node capabilities into their corresponding node's URLs before returning the requested document. The advantage of this method is that clients do not need to be modified: clients use augmented URLs in the same way as they use normal URLs. The drawback of this method is that document servers must parse each requested document.

A problem we have come across with the implementation of the group extension is that clients acquiring more than one group capability cannot tell which one they must use. As the implementation effectuates all authorization exchanges on the HTTP level, the documents do not provide any hint as to what group capability a client should present when following a link. As a consequence, clients have to try their group capabilities one after another until they score a hit. A solution to this problem is to have node servers return unauthorized messages which list all the group names associated with a node. This solution is not practical because popular nodes may be used in several presentation trees. Moreover, clients have to waste a transaction to find out which capability they must use. Another solution is to modify the client so that it remembers which group capability it used when it successfully followed a link. In this way, the client can use the same group capability when following other related links.

7 Related work

This section briefly mentions related work that has been done in the area of coordinated WWW distributed authorization.

DCE Web [13, 14] is an on-going project to marry OSF's Distributed Computing Environment with WWW. DCE Web adds to WWW the advantages of DCE security, which include distributed authentication, consistent group[2] ad-

[2] In DCE, a group is a list of clients who share a set of access rights to a set of objects or services.

ministration across a domain, protection of nodes with ACLs, and remote administration of ACLs. Client authentication is implemented using a conventional key trusted third party scheme derived from Kerberos [22]. Rather than having each server define its own groups, groups are handled by the same third party which handles user authentication. The authentication credentials, which a user retrieves to contact a server, include the user's group attributes. Although DCE Web does not explicitly support coordinated authorization for distributed documents and contents, it provides several tools that can be used to reach that goal. For example, DCE Web's group support can be used to implement our model's group extension using a conventional key cryptosystem.

The Phoenix project [12] is a distributed hypermedia authoring system which integrates access control information to hypermedia documents. Documents are protected by means of ACLs; however, instead of storing the documents together with the ACLs, each document includes an HTML mark-up element giving the URL of an ACL. To authorize document requests, a document server sends the requested method, the ACL URL reference, and the authenticated client-name to an authorization server. The authorization server retrieves the ACL, searches it for an adequate entry, and returns the authorization result to the document server. Authorized users can change both the ACL and the links that point to it in a remote fashion. Phoenix can support coordinated authorization by having different documents share the same ACL. We were not able to find out how Phoenix protects contents or other non-html objects. Compared with Phoenix, our model protects documents without needing to modify them. Authorization in our model is handled locally by each node server whereas Phoenix uses a centralized authorization server. In our model as well as in Phoenix, only one server needs to know its potential clients.

Hyper-G [10, 2] is a second-generation, large-scale distributed hypermedia system which uses an object-oriented database layer to provide, among other features, information-structuring and link-maintenance facilities, as well as a hierarchical access control scheme. Contents are stored outside of the database. Access can be restricted to contents[3], documents, and presentation trees to certain groups of users. Hyper-G also supports the modification of the database by authorized clients. A Hyper-G system comprises a link server and a collection of content servers. The link server is responsible for handling the database and authorizing the client requests. In a typical session, a client authenticates itself to a link server and then sends its node requests to it. Requests can be either for information contained in the database or for contents. In the latter case, it is the link server, and not the client, which contacts the content server and instructs it to send the contents to the client. Both our model and Hyper-G provide authorization at both the presentation tree and document levels. Hyper-G's use of a centralized server allows it to provide even a finer level of authorization granularity. Moreover, the use of a centralized server provides a practical client and database administration. Our model uses a distributed authorization approach. Although our model simplifies client administration, it presents problems when trying to revoke capabilities before their validation period expires. In both models, only one server needs to know its potential clients.

Sessioneer [3] is a recently proposed framework which is close to our authorization model. Sessioneer uses certificates (similar to capabilities) to control access to documents. Clients authenticate once when retrieving a root document. Document servers parse each requested document and embed certificates into the document's outgoing node links. Clients automatically use those certificates when traversing a link. Although some possible attributes of certificates are cited, such as the client's identity, client's IP address, and time stamps, Sessioneer leaves the definition of a certificate format to the applications. This model does not require any modification of clients nor servers. As in our model, user annotations have a limited life. Our model defines a more specific capability format in order to reach the goal of distributed authorization. It should be possible to combine both approaches in order to enjoy the advantages of each.

8 Concluding remarks

We believe that supporting coordinated authorization for distributed documents and contents is an important issue for WWW systems as it will not be always possible to store everything in a single server. By storing nodes according to their types into specialized servers, the overall workload of the system will be better balanced.

We have presented an authorization model that provides coordinated, distributed authorization at the presentation tree and document levels. The use of capabilities as an access-control mechanism simplifies the administration of clients

[3] Hyper-G documents use the term *document* to refer to contents and the term *collection* to refer to either a document or a presentation tree. In order to have a homogeneous terminology, we converted their notation into the one used in this paper.

and distributes the authorization process among different node servers. The model provides both sequential- and non-sequential access modes. The model supports existing WWW node migration techniques. We also explained choices we have made and problems we have encountered while building a prototype of the model. Some solutions to those problems were also proposed.

We believe that our authorization model can be used to protect access to persistent presentation trees when the client population changes at a fast rate; for example, an electronic public library where a client buys access for a limited period.

Other authorization approaches use centralized authorization servers which are consulted each time a client requests a node. A deeper comparison of both distributed and centralized authorization approaches is necessary to know in what situations each one might be better used.

Acknowledgments

The author sincerely thanks the Program Committee of INET'95 for their financial support for publishing and presenting this paper. This work was financed by a grant from CONACyT, a Mexican public institution, and the CCETT, a France Telecom joint research center for broadcast and telecommunications.

References

[1] S. G. Akl, "Digital Signatures: A Survey," tech. report 82-145, Department of Computing and Information Science, Queen's University, Kingston, Ontario, Canada, Now, 1982.

[2] K. Andrews, F. Kappe, and H. Maurer, "Serving Information on the Web with Hyper-G," in *Proc. Third World-Wide Web Conference*, pp. 919-926, Apr. 1995. http://www.igd.fhg.de/www/www95/papers/105/hgw3.html

[3] S. Anderson and R. Garvin, "Sessioneer: Flexible Session Level Authentication with off the Shelf Servers and Clients," In *Proc. Third World-Wide Web Conference*, pp. 1047-1053, Apr. 1995. http://www.igd.fhg.de/www/www95/papers/77/sessioneer2.html

[4] T. Berners-Lee, Hypertext Transfer Protocol, Internet Draft, 5 Nov. 1993 (Expires 5 May 1994).

[5] T. Berners-Lee, Uniform Resource Locators - A unifying syntax for the expression of names and addresses of objects on the network, Internet draft, draft-ietf-uri-url-02.ps. 1 Jan. 1994, expires 1 Jul. 1994.

[6] T. Berners-Lee, R. Cailliau, A. Luotonen, H. Frystik Nielsen, and A. Secret, "The World-Wide Web," Comm. of the ACM, Vol. 37, No. 8, pp. 76-82, Aug. 1994.

[7] European Computer Manufacturers Association, Standard ECMA38: Security in Open Systems - Data Elements and Service Definitions, ECMA, Dec. 1989.

[8] J. Kahan, "Un nouveau modèle d'autorisation pour les systèmes de consultation d'information multimédia répartie," In *Proc. Où, quand, commment protéger vos logiciels et documents électroniques,* AFCET, Dec. 1994. (In French)

[9] J. Kahan, "A Capability-Based Authorization Model for the World-Wide Web," In Proc. *Third World-Wide Web Conference*, pp. 1055-1064, Apr. 1995. http://www.igd.fhg.de/www/www95/papers/86/CAMWWW.html

[10] F. Kappe, Hyper-G Technical Documentation. http://info.iicm.tu-graz.ac.at/Ctechnical

[11] K.-Y. Lam and D. Gollman, "Freshness Assurance of Authentication Protocols," In Proc. *ESORICS 92*, pp. 293-303, 1992.

[12] M. G. Lavenant and J. A. Kruper, "The Phoenix Project:Distributed Hypermedia Authoring," In *Proc. First World-Wide Web Conference*, Spring 1994. http://www.cern.ch/PapersWWW94/j-kruper.ps

[13] S. Lewontin and M. E. Zurko, "The DCE Web Project: Providing Authorization and other Distributed Services to the World-Wide Web," In *Proc. Second World-Wide Web Conference*, 1994. http://www.ncsa.uiuc.edu/SDG/IT94/Proceedings/Security/

[14] S. Lewontin, "The DCE Web Toolkit: Enhancing WWW Protocols with Lower-Layer Services," In *Proc. Third World-Wide Web Conference*, pp. 765-771, Apr. 1995.// http://www.igd.fhg.de/www/www95/papers/67/DCEWebKit.html

[15] M. R. Low and B. Christianson, "Technique for Authentication, Access Control and Re-

source Management in Open Distributed Systems," Electronic Letters, Vol. 30, No. 2, pp. 124-125, 20 Jan. 1994.

[16] R. McCool, Using PGP/PEM Encryption. http://hoohoo.ncsa.uiuc.edu/docs/PEMPGP.html

[17] B. Clifford Neuman, "Proxy-Based Authorization and Accounting for Distributed Systems," In *Proc. 13th Int. Conf. on Dist. Comp. Syst.*, Pittsburgh, pp. 283-291, May 1993.

[18] K. E. Rowe and C. K. Nicholas, "Reliability of WWW name servers," In *Proc. Third World-Wide Web Conference*, pp. 773-783, Apr. 1995. http://www.igd.fhg.de/www/www95/papers/75/rowe_release_2/www-reliable.html

[19] R. S. Sandhu and P. Samarati, ' Access Control: Principles and Practice," IEEE Comm. Magazine, pp. 40-48, Sep. 1994.

[20] J.H. Saltzer and M. D. Schroeder, "The Protection of Information in Computer Systems," Proc.of the IEEE, 63(9), pp. 1278-1308, 1975.

[21] K. Sollins and L. Masinter, Functional Requirements for Uniform Resource Names, draft-ietf-uri-urn-req-01.txt, 14 Oct. 1994.

[22] J. G. Steiner, C. Neuman, and J. I. Schiller, "Kerberos: An Authentication Service for Open Network Systems," In *Proc. Winter USENIX Conf.*, 1988.

[23] V. Varadharajan, P. Allen, and S. Black, "An Analysis of the Proxy Problem in Distributed Systems," In *Proc. IEEE Symp. on Security and Privacy*, pp. 255-275, 1991.

[24] M. E. Zurko and P. M. Hallam-Baker, "Secure Authorization Issues on the Web," In *Tutorial Notes - Third World-Wide Web Conference*, pp. 143-186, Apr., 1995.

Author Information

José Kahan is a PhD candidate in Computer Science at the Université de Rennes I (France). He is working on authorization issues and models for distributed hypermedia consultation services. He holds a specialization degree in Computer Networks from the Ecole Supérieure d'Electricité (France), and a degree in Electronics Engineering from the Universidad Autonoma Metropolitana-Azcapotzalco (Mexico).

Author contact (expires October 1995):

CCETT AMS/ARM
4, rue du Clos-Courtel BP 59
35512 CESSON-SEVIGNE CEDEX
FRANCE

F

[Help] *Last update at http://inet.nttam.com : Fri May 19 15:45:20 1995*

INET'95 Hypermedia Proceedings -- Author Information

Please update and improve your on-line paper

FTP server (ftp.nttam.com) for hypermedia proceedings is available for any correction and addtional materials.

Materials Specification

```
Contents             Preferable Format     FILENAME(example)

Revised paper        tar (HTML and GIF)    012.paper.tar[.Z]
                     HTML                  012.paper.html
                     ASCII text            012.paper.txt
                     GIF                   012.graph1.gif
Your portrait        GIF,200x200 or less   012.picture.gif
Audio for abstract   AU                    012.audio.au
Video clip           QuickTime             012.video.mov
                                           ^^^
                                           XXX=3 digit Paper ID
                                                 [Required]
```

If you can not create a file using data format above, please contact to inet-hmp-sec@nttam.com.

Directions to upload (in case of UNIX)

1. **ftp ftp.nttam.com**.
2. login in as **anonymous**, and enter **your email address** as password
3. **cd post** (move to directory for posting)
4. **binary** (when sending a binary file)
5. **put FILENAME**
6. **quit**

Please do not forget that you cannot overwrite a file of the same name. So at the second time, you may send a file with different name. After uploading a file, please send an email message to inet-hmp-sec@nttam.com.

Thank you.

---

inet95@nttam.com